

Aperio GT 450 DX

Podręcznik kierownika IT i administratora laboratorium



Aperio GT 450 DX Przewodnik dla kierownika IT i administratora laboratorium

Ten dokument dotyczy sterownika Aperio GT 450 DX, konsoli Aperio GT 450 DX i modułu Aperio GT 450 DX SAM DX w wersji 1.1 i nowszych.


Informacje dotyczące praw autorskich


- ▶ Copyright © 2022 Leica Biosystems Imaging, Inc. Wszelkie prawa zastrzeżone. LEICA i logo Leica są zastrzeżonymi znakami towarowymi firmy Leica Microsystems IR GmbH. Aperio, GT i GT 450 są znakami towarowymi Leica Biosystems Imaging w USA i opcjonalnie w innych krajach. Inne logo, nazwy produktów i/lub firm mogą być znakami towarowymi należącymi do ich właścicieli.
- ▶ Ten produkt jest chroniony zarejestrowanymi patentami. Aby uzyskać wykaz patentów, należy skontaktować się z firmą Leica Biosystems.

Materiały dla klientów

- ▶ Najnowsze informacje na temat produktów i usług Aperio firmy Leica Biosystems można znaleźć na stronie www.LeicaBiosystems.com/Aperio.

Dane kontaktowe – Leica Biosystems Imaging, Inc.

Siedziba główna	Obsługa klienta	Informacje ogólne
 Leica Biosystems Imaging, Inc. 1360 Park Center Drive Vista, CA 92081 USA Tel: +1 (866) 478-4111 (numer bezpłatny) Bezpośredni międzynarodowy nr tel.: +1 (760) 539-1100	W tej części opisano zalecany sposób kontaktowania się z lokalnym przedstawicielem pomocy technicznej w przypadku wszelkich zapytań i zgłoszeń serwisowych. https://www.leicabiosystems.com/service-support/technical-support/	USA/Kanada, nr tel.: +1 (866) 478-4111 (numer bezpłatny) Bezpośredni międzynarodowy nr tel.: +1 (760) 539-1100 Adres e-mail: ePathology@LeicaBiosystems.com

Autoryzowany przedstawiciel w Unii Europejskiej	Osoba odpowiedzialna w Wielkiej Brytanii
 CEpartner4U Esdoornlaan 13 3951 DB Maarn Holandia	Leica Microsystems (UK) Limited Larch House, Woodlands Business Park Milton Keynes, Anglia, Wielka Brytania, MK14 6FG

Importerzy	
 Leica Biosystems Deutschland GmbH Heidelberger Straße 17-19 69226 Nussloch, Niemcy	Leica Microsystems (UK) Limited Larch House, Woodlands Business Park Milton Keynes, Anglia, Wielka Brytania, MK14 6FG



UDI 00815477020297, 00815477020389

REF 23GT450DXIVD, 23SAMSWDXIVD

Spis treści

Uwagi	5
Rejestr wersji	5
Przestrogi i uwagi	5
Symbole	6
Dane kontaktowe działów obsługi klienta	8
1 Wstęp.....	10
Informacje na temat podręcznika	11
Powiązane dokumenty.....	12
Logowanie do SAM DX	12
Interfejs użytkownika SAM DX	13
2 Architektura sieci skanera Aperio GT 450 DX	15
Obsługiwane typy obrazów	15
Informacje ogólne	15
Wymogi dotyczące przepustowości sieci.....	16
W jaki sposób skaner Aperio GT 450 DX dostosowuje się do posiadanej sieci	16
Bezpieczny dostęp	16
Zalecana konfiguracja sieci dla skanera Aperio GT 450 DX	17
3 Konfiguracja skanera Aperio GT 450 DX	19
Instrukcje ogólne	19
Podstawowe ustawienia skanera	20
Scanner System Information: Info Page (Informacje o systemie skanera: Strona informacji)	21
Scanner System Information: Settings Page (Informacje o systemie skanera: Strona ustawień)	22
Scanner Configuration Settings (Ustawienia konfiguracji skanera)	23
Strona obrazów	25
Format nazwy pliku obrazu	26
Zarządzanie kodami kreskowymi	26
Zarządzanie kodami PIN.....	27
Konfigurowanie kodu PIN i Timeout (Limit czasu)	27
Aktywowanie wyjścia obrazów DICOM.....	28

4	Wyświetlanie informacji o systemie	30
	Wyświetlanie informacji o skanerze i ustawień	30
	Wyświetlanie statystyk dotyczących skanera	31
	Obsługa dziennika zdarzeń	32
	Tworzenie kopii zapasowej plików dziennika	32
	Alerty logowania	32
5	Zarządzanie użytkownikami	33
	Rozumienie roli	33
	Zarządzanie użytkownikami	34
	Dodawanie użytkownika	34
	Edytowanie użytkownika	35
	Usuwanie użytkownika	35
	Odblokowanie konta użytkownika	35
	Zmiana hasła użytkownika	36
6	Wtyczne dotyczące cyberbezpieczeństwa i sieci	37
	Funkcje cyberbezpieczeństwa skanera Aperio GT 450 DX i aplikacji Aperio SAM DX	37
	Ochrona danych	38
	Fizyczne zabezpieczenia skanera Aperio GT 450 DX	38
	Ochrona serwera SAM DX	38
	Ochrona za pomocą hasła, loginu i konfiguracji użytkownika	38
	Fizyczne zabezpieczenia dla serwera SAM DX	39
	Zabezpieczenia administracyjne serwera SAM DX	39
	Korzystanie z gotowego, komercyjnie dostępnego oprogramowania	40
	Obsługa i poprawki cyberbezpieczeństwa	40
A	Rozwiązywanie problemów	41
	Rozwiązywanie problemów związanych z aplikacją Scanner Administration Manager DX (SAM DX)	41
	Uruchomić ponownie DataServer	42
	Sprawdzić, czy Mirth działa	42
	Błąd konfiguracji IIS	42
B	Zestawienie ustawień skanera i opcji konfiguracji	43
	Podstawowe informacje o skanerze	43
	Konfiguracja skanera	44
C	Wiązanie certyfikatu SSL z Aperio SAM DX	46
	Przypisywanie certyfikatu SSL do witryny internetowej	46
	Wiązanie certyfikatu SSL	47
	Indeks	50

Uwagi

Rejestr wersji

Wer.	Data wydania	Sekcje objęte aktualizacją	Szczegóły
B	Maj 2022	Maj 2022	Poprawiono kilka błędów typograficznych.
A	Kwiecień 2022	Wszystkie	Nowa wersja dla produktu Aperio GT 450 DX. Na podstawie istniejącego dokumentu <i>Aperio GT 450 DX Przewodnik dla kierownika IT i administratora laboratorium MAN-0459</i> , Wersja B. Nie przetłumaczone.

Przestrogi i uwagi

- ▶ **Zgłaszanie poważnych incydentów** – Wszelkie poważne incydenty związane z Aperio GT 450 DX należy zgłaszać producentowi i właściwym organom państwa członkowskiego, w którym ma siedzibę użytkownik i/lub pacjent.
- ▶ **Specyfikacje i działanie** – Specyfikacje i opis działania urządzenia znajdują się w dokumencie *Specyfikacje skanera Aperio GT 450 DX*.
- ▶ **Instalacja** – Aperio GT 450 DX musi być zainstalowany przez przeszkolonego przedstawiciela działu usług technicznych firmy Leica Biosystems.
- ▶ **Naprawa** – Naprawy mogą być wykonywane wyłącznie przez przeszkolonego przedstawiciela działu usług technicznych firmy Leica Biosystems. Po wykonaniu naprawy należy poprosić technika firmy Leica Biosystems o przeprowadzenie kontroli, aby upewnić się, czy produkt działa prawidłowo.
- ▶ **Akcesoria** – Aby uzyskać informacje na temat używania Aperio GT 450 DX z akcesoriami innych firm, takimi jak Laboratory Information System (LIS), które nie zostały dostarczone przez firmę Leica Biosystems, należy skontaktować się z przedstawicielem działu usług technicznych Leica Biosystems.
- ▶ **Kontrola jakości** – Informacje na temat kontroli jakości obrazu znajdują się w *Podręczniku użytkownika Aperio GT 450 DX*.
- ▶ **Konserwacja i rozwiązywanie problemów** – Informacje na temat konserwacji znajdują się w *Podręczniku użytkownika Aperio GT 450 DX*.
- ▶ **Cyberbezpieczeństwo** – Należy pamiętać, że stacje robocze i serwery są podatne na złośliwe oprogramowanie, wirusy, uszkodzenie danych i naruszenia prywatności. Należy współpracować z administratorami systemów informatycznych, aby chronić stację roboczą poprzez przestrzeganie polityki w zakresie haseł i bezpieczeństwa instytucji.















Zalecenia Aperio dotyczące ochrony serwera SAM DX znajdują się tutaj „Rozdział 6: Wytyczne dotyczące cyberbezpieczeństwa i sieci” na stronie 37.




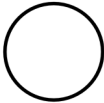




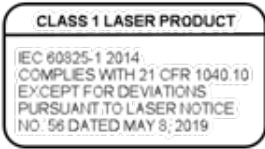
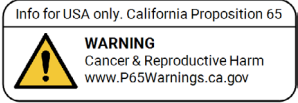
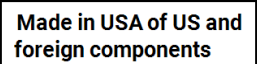
W przypadku wykrycia podejrzanego luki lub incydentu związanego z bezpieczeństwem cybernetycznym Aperio GT 450 DX należy skontaktować się z działem technicznym Leica Biosystems w celu uzyskania pomocy.

- ▶ **Szkolenie** – Niniejsza instrukcja nie może zastąpić szczegółowego szkolenia dla operatorów przeprowadzanego przez firmę Leica Biosystems ani innych zaawansowanych instrukcji.
- ▶ **Bezpieczeństwo** – Jeżeli urządzenie będzie używane w sposób niezgodny z zaleceniami producenta, może dojść do naruszenia bezpieczeństwa.

Symbole

Na etykiecie produktu lub w niniejszym podręczniku użytkownika pojawiają się poniższe symbole.

Symbol	Rozporządzenie/ norma	Opis
	ISO 15223-1 - 5.4.3	Zapoznać się z instrukcją obsługi.
	ISO 15223-1 - 5.1.1	Producent
	ISO 15223-1 - 5.1.3	Data produkcji
	ISO 15223-1 - 5.1.2	Autoryzowany przedstawiciel w Unii Europejskiej
	ISO 15223-1 - 5.1.8	Importer
	AS/NZS 4417.1	Urządzenie jest zgodne z wymaganiami australijskiego organu ds. środków komunikacji (Australian Communications Media Authority, ACMA) (bezpieczeństwo i kompatybilność elektromagnetyczna) w Australii i Nowej Zelandii.
	ISO 15223-1 - 5.1.7	Numer seryjny
	ISO 15223-1 - 5.5.1	Urządzenia medyczne do diagnostyki in vitro.
	ISO 15223-1 - 5.1.6	Numer katalogowy
	ISO 15223-1 - 5.7.10	Unikalny identyfikator urządzenia
	EU 2017/746 Artykuł 18	Urządzenie ma znak CE (Conformité Européenne) i spełnia wymagania Rozporządzenia UE 2017/746.
	Rozporządzenia w sprawie wyrobów medycznych 2002	Urządzenie jest zgodne z wymaganiami Oceny zgodności Wielkiej Brytanii (UK Conformity Assessment).
	ISO 15223-1 - 5.4.4	Zachować ostrożność
	SO 7010 - W001	Ogólne ostrzeżenie

Symbol	Rozporządzenie/ norma	Opis
	IEC 61010-1	Firma TÜV Product Services poświadczyła, że wymienione produkty są zgodne z wymaganiami bezpieczeństwa obowiązującymi w USA i Kanadzie.
	IEC 60417 - 5031	To urządzenie może być zasilane wyłącznie prądem stałym.
	IEC 60417 - 5007	Wł. W celu wskazania podłączenia do sieci elektrycznej, przynajmniej w odniesieniu do przełączników sieci elektrycznej lub ich pozycji, i sytuacji związanych z bezpieczeństwem.
	IEC 60417 - 5008	Wył. W celu wskazania odłączenia od sieci elektrycznej, przynajmniej w odniesieniu przełączników sieci elektrycznej lub ich pozycji, i wszystkich sytuacji związanych z bezpieczeństwem.
	ISO 15523-1 5.7.3	Ograniczenie temperatury
	ISO 15223-1 5.3.8	Ograniczenia dotyczące wilgotności
	2012/19/UE	Urządzenie podlega Dyrektywie 2012/19/UE (WEEE) w sprawie zużytego sprzętu elektrycznego i elektronicznego i jego utylizacja podlega specjalnym warunkom.
	Norma dla przemysłu elektronicznego Chińskiej Republiki Ludowej SJ/T11364 (People's Republic of China Electronic Industry Standard SJ/T11364)	Urządzenie zawiera pewne toksyczne lub niebezpieczne elementy i może być użytkowane bezpiecznie w trakcie okresu, gdy jego użytkowanie jest bezpieczne dla środowiska. Numer na środku logo wskazuje bezpieczny dla środowiska okres użytkowania produktu (w latach). Zewnętrzny okrąg wskazuje, że produkt może zostać poddany recyklingowi.
	IEC 60825-1	Urządzenie jest produktem laserowym klasy 1, spełniającym międzynarodowe normy i wymagania obowiązujące w USA.
	CA Proposition 65	Ten produkt może wystawiać użytkownika na działanie substancji chemicznych znanych w stanie Kalifornia, które mogą być rakotwórcze i szkodliwe dla rozrodczości. Dodatkowe informacje można uzyskać na stronie https://www.P65Warnings.ca.gov .
	Nie dot.	Urządzenie zostało wyprodukowane w USA z komponentów wytwarzanych w USA i w innych krajach.

Dane kontaktowe działów obsługi klienta

W celu uzyskania pomocy technicznej prosimy o kontakt z biurem w danym kraju.

Australia:

96 Ricketts Road
Mount Waverly, VIC 3149
AUSTRALIA
Tel: 1800 625 286 (numer bezpłatny)
Od 8:30 do 17:00, od poniedziałku do piątku, AEST
Adres e-mail: lbs-anz-service@leicabiosystems.com

Austria:

Leica Biosystems Nussloch GmbH
Technical Assistance Center
Heidelberger Strasse 17
Nussloch 69226
NIEMCY
Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +43 1 486 80 50 50
Adres e-mail: support.at@leicabiosystems.com

Belgia:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +32 2 790 98 50
Adres e-mail: support.be@leicabiosystems.com

Kanada:

Tel: +1 844 534 2262 (numer bezpłatny)
Bezpośredni międzynarodowy nr tel.: +1 760 539 1150
E-mail: TechServices@leicabiosystems.com

Chiny:

17F, SML Center No. 610 Xu Jia Hui Road, Huangpu
District
Szanghaj, PRC PC:200025
CHINY
Tel: +86 4008208932
Faks: +86 21 6384 1389
Adres e-mail: service.cn@leica-microsystems.com
Adres e-mail opieki zdalnej: tac.cn@leica-microsystems.com

Dania:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +45 44 54 01 01
Adres e-mail: support.dk@leicabiosystems.com

Niemcy:

Leica Biosystems Nussloch GmbH
Technical Assistance Center
Heidelberger Strasse 17
Nussloch 69226
NIEMCY
Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +49 6441 29 4555
Adres e-mail: support.de@leicabiosystems.com

Irlandia:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +44 1908 577 650
Adres e-mail: support.ie@leicabiosystems.com

Hiszpania:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +34 902 119 094
Adres e-mail: support.spain@leicabiosystems.com

Francja:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +33 811 000 664
Adres e-mail: support.fr@leicabiosystems.com

Włochy:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +39 0257 486 509
Adres e-mail: support.italy@leicabiosystems.com

Japonia:

1-29-9 Takadanobaba, Shinjuku-ku
Tokio 169-0075
JAPONIA

Holandia:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +31 70 413 21 00
Adres e-mail: support.nl@leicabiosystems.com

Nowa Zelandia:

96 Ricketts Road
Mount Waverly, VIC 3149
AUSTRALIA
Tel: 0800 400 589 (numer bezpłatny)
Od 8:30 do 17:00, od poniedziałku do piątku, AEST
Adres e-mail: lbs-anz-service@leicabiosystems.com

Portugalia:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +35 1 21 388 9112
Adres e-mail: support.pt@leicabiosystems.com

Federacja Rosyjska

BioLine LLC
Pinsky lane 3 letter A
Saint Petersburg 197101
FEDERACJA ROSYJSKA
Tel: 8-800-555-49-40 (numer bezpłatny)
Tel. krajowy: +7 812 320 49 49
Adres e-mail: main@bioline.ru

Szwecja:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +46 8 625 45 45
Adres e-mail: support.se@leicabiosystems.com

Szwajcaria:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +41 71 726 3434
Adres e-mail: support.ch@leicabiosystems.com

Zjednoczone Królestwo:

Tel: 0080052700527 (numer bezpłatny)
Tel. krajowy: +44 1908 577 650
Adres e-mail: support.uk@leicabiosystems.com

USA:

Tel: +1 844 534 2262 (numer bezpłatny)
Bezpośredni międzynarodowy nr tel.: +1 760 539 1150
E-mail: TechServices@leicabiosystems.com

1

Wstęp

Niniejszy rozdział przedstawia aplikację Scanner Administration Manager DX (SAM DX) do użytkowania z jednym skanerem lub wieloma skanerami Aperio GT 450 DX.

Aperio GT 450 DX jest skanerem korzystającym z metody jasnego pola do wykonywania skanów całych szkiełek mikroskopu z funkcją ciągłego ładowania z maksymalną pojemnością 450 szkiełek na 15 koszykach, oferującym możliwość ustawiania priorytetowych koszyków do skanowania, automatyczną kontrolę jakości obrazu i prędkość skanowania ~32 sekund przy 40-krotnym powiększeniu skanowania dla obszaru 15 mm x 15 mm. Skaner Aperio GT 450 DX został zaprojektowany w taki sposób, aby był dopasowany do środowiska sieciowego i oferował najwyższe bezpieczeństwo i najlepszą wydajność.

Urządzenie Aperio GT 450 DX może być użytkowane przez przeszkolonych klinicznych techników histopatologii, podczas gdy oprogramowanie urządzenia Aperio GT 450 DX przeznaczone jest dla profesjonalistów IT i administratorów laboratoriów.

Urządzenie Aperio GT 450 DX przeznaczone jest dla średnich lub dużych laboratoriów patologicznych, które świadczą usługi z zakresu patologii dla szpitali, laboratoriów referencyjnych lub innych placówek klinicznych.

Należy stosować prawidłowe praktyki laboratoryjne oraz zasady i procedury wymagane przez instytucję w zakresie przygotowywania, przetwarzania, przechowywania i utylizacji szkiełek. Niniejsze urządzenie może być użytkowane jedynie w celach i w sposób opisany w *Podręczniku użytkownika skanera Aperio GT 450 DX*.

Element	Opis
Serwer Scanner Administration Manager DX (SAM DX)	Serwer SAM DX łączy się z wieloma skanerami Aperio GT 450 DX i obsługuje oprogramowanie aplikacji klienta SAM DX.
Oprogramowanie aplikacji klienta Scanner Administration Manager DX (SAM DX)	Oprogramowanie aplikacji klienta SAM DX umożliwia wdrożenie w systemie informatycznym, konfigurację kodu PIN i obsługę wielu skanerów z poziomu jednego klienta stacjonarnego dla profesjonalnych informatyków.
Stacja robocza, monitor i klawiatura	Stacja robocza, monitor i klawiatura muszą zostać podłączone do lokalnej sieci (LAN) z dostępem do serwera SAM DX, aby możliwe było obsługiwanie skanerów GT 450 DX za pomocą aplikacji SAM DX.

Urządzenie Aperio GT 450 DX zawiera aplikację Scanner Administration Manager DX (SAM DX), która umożliwia jego wdrożenie w systemie informatycznym i dostęp serwisowy dla maksymalnie 4 skanerów z jednej stacjonarnej stacji klienta. Aplikacja SAM DX usprawnia procedurę ustawień, konfiguracji i monitorowania każdego skanera. Aplikacja SAM DX instalowana jest na serwerze, znajdującym się w tej samej sieci, co skaner/skanery, jak również inne komponenty do zarządzania obrazami.

Funkcjami SAM DX są:

- ▶ Internetowy interfejs użytkownika, kompatybilny z większością obecnie dostępnych przeglądarek, umożliwia dostęp w całej sieci placówki.
- ▶ Dostęp użytkowników oparty na rolach. Rola Operatora umożliwia użytkownikom wyświetlanie ustawień konfiguracji, podczas gdy rola administratora pozwala użytkownikowi na zmianę ustawień.
- ▶ Specyficzne dla skanera ustawienia konfiguracji dla kodów PIN dostępu użytkownika i limitów czasu. Dla każdego skanera w systemie można skonfigurować oddzielny kod PIN.
- ▶ Centralne wyświetlanie statystyk i dzienników zdarzeń. Informacje dla każdego skanera w systemie można wyświetlić i przeglądać z poziomu interfejsu SAM DX w celu ich porównania.
- ▶ Obsługa wielu skanerów ze scentralizowaną konfiguracją i monitoringiem.
- ▶ Natychmiastowe wyświetlanie stanu skanera. Strona główna wyświetla, które skanery są online, a które nie.
- ▶ Usługi przetwarzania danych dziennika i zdarzeń poprzez serwer Mirth Connect, podłączony do bazy danych w systemie plików.

Informacje na temat podręcznika

Niniejszy podręcznik skierowany jest do administratorów laboratoriów, kierowników działów informatycznych i pozostałych osób odpowiedzialnych za zarządzanie urządzeniem Aperio GT 450 DX w sieci danej placówki. Ogólne informacje dotyczące użytkownika skanera znajdują się w *Podręczniku użytkownika skanera Aperio GT 450 DX*.

Kolejny rozdział niniejszego podręcznika objaśnia architekturę sieciową skanera Aperio GT 450 DX i przedstawia przepływ danych pomiędzy różnymi elementami systemu.

Następne rozdziały omawiają obsługę aplikacji Scanner Administration Manager DX (SAM DX) w celu skonfigurowania skanera/skanerów Aperio GT 450 DX, w tym sposób dodawania kont użytkowników do aplikacji SAM DX i konfiguracji dostępowych kodów PIN dla każdego skanera. Zadania dostępne wyłącznie dla personelu pomocy technicznej firmy Leica są poza zakresem niniejszego podręcznika.

Informacje dotyczące określonych zadań znajdują się w tabeli poniżej.

Zadanie	Zobacz...
Dowiedz się, w jaki sposób skanery GT 450 DX i serwer aplikacji Scanner Administration Manager DX (SAM DX) dostosowują się do posiadanej sieci	<i>„Rozdział 2: Architektura sieci skanera Aperio GT 450 DX” na stronie 15</i>
Dowiedz się, jak odbywa się przepływ danych pomiędzy skanerem Aperio GT 450 DX, serwerem SAM DX i opcjonalnymi serwerami obrazów i do zarządzania danymi.	<i>„Zalecana konfiguracja sieci dla skanera Aperio GT 450 DX” na stronie 17</i>
Należy zalogować się do oprogramowania aplikacji klienta Scanner Administration Manager DX (SAM DX)	<i>„Logowanie do SAM DX” na stronie 12</i>
Dostosowywanie ustawień konfiguracji dla komunikacji pomiędzy DICOM lub DSR i serwerem SAM DX i skanerem	<i>„Scanner Configuration Settings (Ustawienia konfiguracji skanera)” na stronie 23</i>
Wyświetlanie informacji o skanerze w systemie	<i>„Rozdział 3: Konfiguracja skanera Aperio GT 450 DX” na stronie 19</i>

Zadanie	Zobacz...
Sprawdzanie, czy skaner jest online	„Interfejs użytkownika SAM DX” na stronie 13
Wyświetlanie numeru seryjnego, wersji oprogramowania lub wersji oprogramowania układowego dla skanera w systemie	„Scanner System Information: Info Page (Informacje o systemie skanera: Strona informacji)” na stronie 21
Przeglądanie statystyk i historii skanera	„Wyświetlanie statystyk dotyczących skanera” na stronie 31
Przeglądanie zaawansowanych opcji konfiguracji, takich jak ustawienia kamery	„Wyświetlanie informacji o skanerze i ustawień” na stronie 30
Dodawanie nowego użytkownika aplikacji Scanner Administration Manager DX (SAM DX)	„Dodawanie użytkownika” na stronie 34
Usuwanie kont użytkowników z SAM DX	„Usuwanie użytkownika” na stronie 35
Zmiana hasła użytkownika	„Zmiana hasła użytkownika” na stronie 36
Odblokowywanie zablokowanego konta użytkownika	„Odblokowanie konta użytkownika” na stronie 35
Diagnostyka problemu poprzez przeglądanie dzienników zdarzeń i błędów	„Obsługa dziennika zdarzeń” na stronie 32
Sprawdzanie dostępności aktualizacji oprogramowania	„Wyświetlanie informacji o skanerze i ustawień” na stronie 30
Przeglądanie zaleceń z zakresu cyberbezpieczeństwa i sieci dla skanera Aperio GT 450 DX	„Rozdział 6: Wytyczne dotyczące cyberbezpieczeństwa i sieci” na stronie 37

Powiązane dokumenty

Filmy dostępne za pośrednictwem ekranu dotykowego skanera Aperio GT 450 DX dostarczają instrukcji dotyczących podstawowych zadań w ramach skanowania, takich jak załadunek i rozładunek koszyków.

Dodatkowe informacje dotyczące obsługi skanera Aperio GT 450 DX znajdują się w poniższych dokumentach:

- ▶ *Krótki przewodnik Aperio GT 450 DX* – podstawowe informacje o obsłudze skanera Aperio GT 450 DX.
- ▶ *Instrukcja obsługi Aperio GT 450 DX* – dodatkowe informacje o skanerze Aperio GT 450 DX.
- ▶ *Specyfikacje Aperio GT 450 DX* – szczegółowe specyfikacje skanera Aperio GT 450 DX.

Logowanie do SAM DX

Po zainstalowaniu i skonfigurowaniu skanera Aperio GT 450 DX kolejnym krokiem jest użycie aplikacji Scanner Administration Manager DX (SAM DX) do skonfigurowania skanerów Aperio GT 450 DX i użytkowników.

1. Otworzyć przeglądarkę internetową i wprowadzić adres serwera SAM DX. (Przedstawiciel instalacyjny firmy Leica przekazuje ten adres przedstawicielowi działu informatycznego w placówce w trakcie instalacji systemu. Należy skontaktować się z personelem działu informatycznego, aby uzyskać ten adres).
2. Wprowadzić nazwę loginu (użytkownika) i hasło. Jeśli użytkownik loguje się po raz pierwszy, należy użyć danych do logowania przekazanych przez administratora systemu lub instalatora firmy Leica Biosystems.
3. Kliknąć opcję **Log In** (zaloguj).

Interfejs użytkownika SAM DX

Poniżej ukazana jest strona główna aplikacji SAM DX z listą skanerów. Należy mieć na uwadze, że użytkownicy z rolą Operator nie widzą ikon Configuration (Konfiguracja).

Scanner Name	Type	System Information	Event Logs	Configuration	Status
Scanner Lab 1	Aperio GT 450 DX	System Information	Event Logs	Configuration	ONLINE
Scanner Lab 2	Aperio GT 450 DX	System Information	Event Logs	Configuration	ONLINE
PathLab 1	Aperio GT 450 DX	System Information	Event Logs	Configuration	OFFLINE
PathLab 2	Aperio GT 450 DX	System Information	Event Logs	Configuration	OFFLINE

Poniżej opisano cztery główne obszary strony.

SCANNERS (4)

- Scanner Lab 1
Aperio GT 450 DX
- Scanner Lab 2
Aperio GT 450 DX
- PathLab 1
Aperio GT 450 DX
- PathLab 2
Aperio GT 450 DX

Lista skanerów

Lista wyświetla każdy skaner w systemie wraz z niestandardową lub „przyjazną” nazwą i modelem skanera. Lab Admin (Administrator laboratorium) mogą kliknąć nazwę skanera w tym obszarze, aby wyświetlić opcje Edit Scanner (Edytuj skaner).

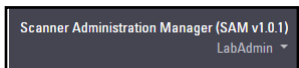
ONLINE

ONLINE

OFFLINE

Obszar stanu skanera

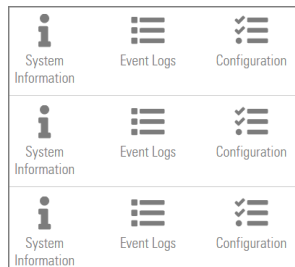
Ten obszar wyświetla status każdego skanera.



Login użytkownika

Wyświetla nazwę użytkownika dla bieżącego użytkownika aplikacji SAM DX.

Należy wybrać nazwę loginu, aby wyświetlić łącza do zmiany hasła i wylogowania.



Obszar poleceń

W tym obszarze znajdują się ikony używane do wyświetlania stron System Information (Informacje o systemie), Event Log (Dziennik zdarzeń) i Configuration (Konfiguracja).

Należy mieć na uwadze, że ikony konfiguracji dostępne są jedynie dla użytkowników z rolą Lab Admin (Administrator laboratorium).

2

Architektura sieci skanera Aperio GT 450 DX

Ten rozdział prezentuje ogólne informacje na temat tego, w jaki sposób skaner Aperio GT 450 DX i serwer SAM DX dostosowują się do posiadanej sieci.

i Awaria sieci informatycznej może opóźnić diagnozę/prognozę do momentu przywrócenia sprawności sieci.

Architektura skanera Aperio GT 450 DX

Skaner Aperio GT 450 DX został zaprojektowany z myślą o łatwości użytkowania w środowisku informatycznym i bezpieczeństwie. Jest gotowy na integrację z posiadanym systemem zarządzania obrazami i danymi (IDMS), LIS i innymi systemami sieciowymi.

Zestaw Aperio GT 450 DX obejmuje skaner Aperio GT 450 DX, serwer aplikacji Scanner Administration Manager DX (SAM DX), kable i wtyczki. Każda instancja serwera SAM DX może obsługiwać cztery skanery Aperio GT 450 DX, a w sieci działać może wiele serwerów SAM DX.

Oprogramowanie aplikacji klienta SAM DX znajduje się na serwerze SAM DX i zawiera następujące:

- ▶ Oprogramowanie SAM DX do konfigurowania skanera
- ▶ Internetowy interfejs użytkownika do zarządzania skanerem i konfigurowania go
- ▶ Usługi logowania i wysyłania komunikatów dotyczących zdarzeń i błędów
- ▶ Serwer DICOM do konwertowania plików obrazów DICOM do formatu SVS i przesyłania ich do systemu przechowywania obrazów

Obsługiwane typy obrazów

Skaner Aperio GT 450 DX tworzy pliki SVS lub obrazy DICOM. Domyślnym formatem obrazów jest .SVS.

Zanim możliwe będzie aktywowanie tworzenia obrazów DICOM, środowisko informatyczne musi spełniać wymagania wymienione w *Deklaracji zgodności z DICOM firmy Aperio*. Ponadto przedstawiciel działu pomocy technicznej firmy Leica Biosystems musi zalogować się do aplikacji SAM DX jako Leica Admin (administrator Leica) i włączyć Optional Features (Opcjonalne funkcje) skanera, aby umożliwić konfigurację DICOM. Szczegółowe informacje podano tutaj: „*Aktywowanie wyjścia obrazów DICOM*” na stronie 28.

Informacje ogólne

Zastosowanie mają następujące wytyczne:

- ▶ Udział sieciowy, w którym obrazy są przechowywane (DSR), może być obecny na tym samym serwerze, co IDMS, lub znajdować się w dowolnym miejscu lokalnej sieci.

- ▶ Obsługa komunikatów obejmuje instancję Mirth Connect i wdrożenie różnych kanałów do przekształcania i trasowania komunikatów skanera (zdarzeń i dzienników związanych ze skanowaniem).

Przed zainstalowaniem skanerów Aperio GT 450 DX, oprogramowania aplikacji klienta SAM DX i serwera SAM DX przedstawiciel działu technicznego firmy Leica Biosystems określa najlepszą architekturę instalacji w oparciu o planowane użytkowanie, bieżącą konfigurację sieci i inne czynniki. Obejmuje to podjęcie decyzji na temat instalacji komponentów na poszczególnych serwerach fizycznych w sieci. Różne komponenty i usługi można zainstalować na różnych serwerach lub na jednym serwerze.

Wymogi dotyczące przepustowości sieci

Połączenie pomiędzy skanerem Aperio GT 450 DX i serwerem SAM DX należy nawiązać poprzez sieć Ethernet o przepustowości 1 gigabita na sekundę (Gb/s) lub większej. W przypadku połączenia pomiędzy serwerem SAM DX i repozytorium obrazów (DSR) wymagana minimalna przepustowość wynosi 10 gigabitów na sekundę.


W jaki sposób skaner Aperio GT 450 DX dostosowuje się do posiadanej sieci

Poniżej przedstawiono najważniejsze komponenty skanera Aperio GT 450 DX i systemu SAM DX:

- ▶ **Aperio GT 450 DX** – Do serwera SAM DX poprzez sieć można podłączyć jeden skaner lub większą ilość skanerów Aperio GT 450 DX. Każdy serwer SAM DX może obsługiwać wiele skanerów.
- ▶ **Serwer aplikacji Scanner Administration Manager DX (SAM DX)** – Serwer SAM DX zawiera oprogramowanie aplikacji klienta Scanner Administration Manager, przedmiot niniejszego podręcznika. Serwer SAM DX zawiera konwerter obrazów DICOM, służący do przekształcania obrazów DICOM do formatu plików obrazów SVS. (Skanery Aperio GT 450 DX przesyłają strumieniowo szyfrowane obrazy DICOM do serwera SAM DX). Serwer SAM DX również zarządza ustawieniami konfiguracji skanera i obsługą wiadomości za pomocą połączeń Mirth.
- ▶ **Serwer Digital Slide Repository (DSR)** – Ten serwer (znany również jako serwer systemu przechowywania obrazów) zawiera wszystkie obrazy szkiełek ze skanera oraz infrastrukturę do zarządzania nimi. Repozytorium może być udziałem sieciowym, dostępnym poprzez serwer w sieci, lub może znajdować się na opcjonalnym serwerze Aperio eSlide Manager.
- ▶ **Stacja robocza/konsola SAM DX** – Dostępne z poziomu przeglądarki internetowej (Firefox, Chrome lub Edge) na komputerze PC lub laptopie w sieci, administratorzy i operatorzy używają konsoli do przeglądania danych zdarzeń i statystyk. Administratorzy mogą również dodawać konta użytkowników, konfigurować kody PIN i wprowadzać zmiany w konfiguracji.
- ▶ **Baza danych** – MS SQL Server Database (Baza danych serwera MS SQL), która zawiera dane użytkowników, dane dotyczące ustawień, dane i zdarzenia raportowane poprzez raporty statystyczne, a także błędy raportowane w dziennikach.
- ▶ **Sieciowy udział plików** – Lokalizacja w posiadanej sieci, w której przechowywane są dzienniki zdarzeń.

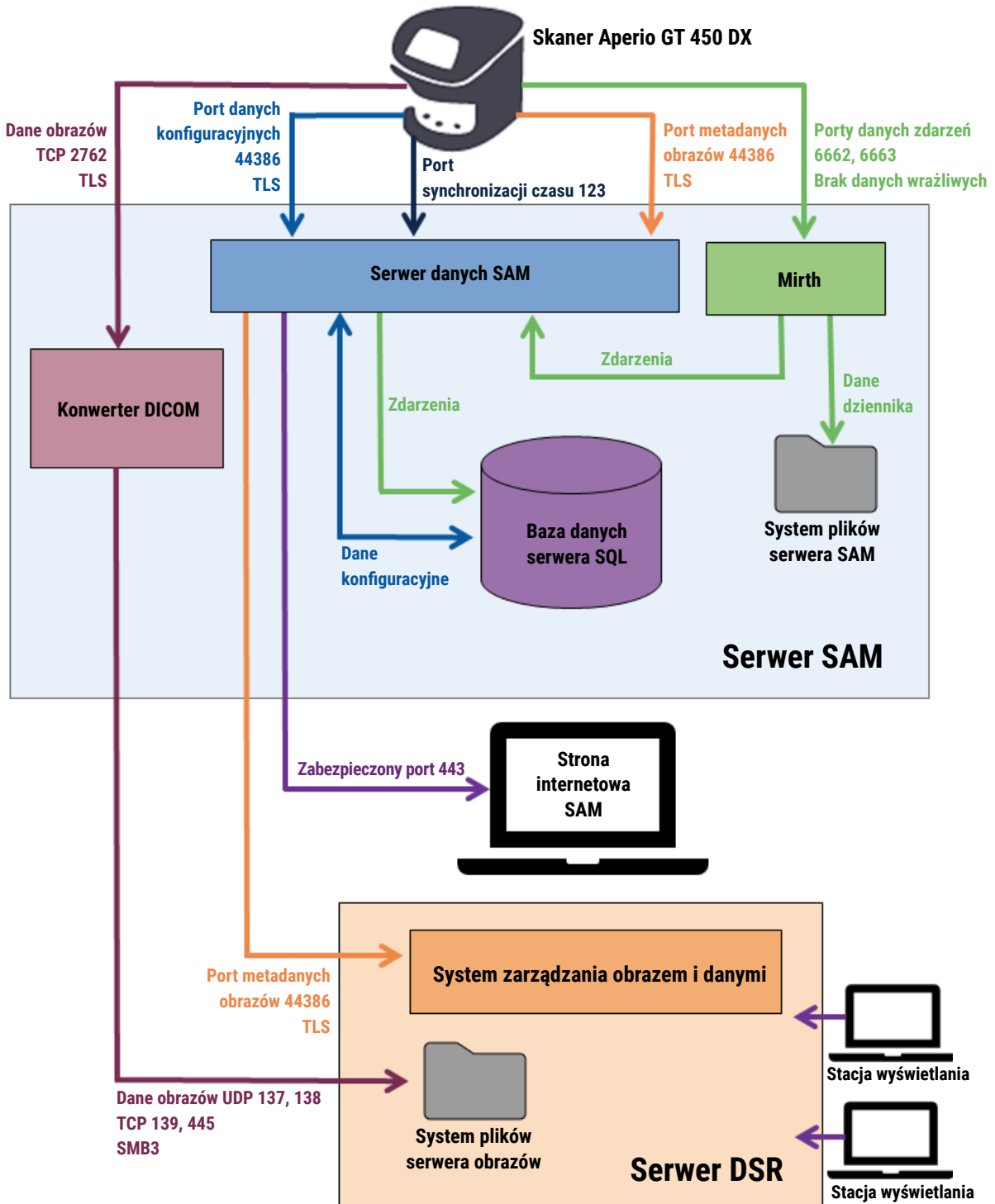
Bezpieczny dostęp

Dostęp poprzez interfejs użytkownika SAM DX jest zabezpieczony protokołem SSL. Certyfikaty SSL z podpisem własnym przekazywane są w trakcie instalacji. Aby uniknąć komunikatów bezpieczeństwa ze strony przeglądarki, klienci mogą zastosować własne certyfikaty bezpieczeństwa.

 Aby zabezpieczyć sieć przed atakami cybernetycznymi, zalecamy wyłączenie nieużywanych portów i usług w sieci.

Zalecana konfiguracja sieci dla skanera Aperio GT 450 DX

Niniejsza sekcja opisuje zalecany sposób łączenia skanera Aperio GT 450 DX w środowisku informatycznym w celu uzyskania optymalnej wydajności.



Typ danych	Opis	Port
Dane obrazów	<p>Skaner wysyła dane obrazu w formacie DICOM do konwertera DICOM. Dane wysyłane są z użyciem szyfrowania TLS.</p> <p>Komunikację pomiędzy skanerem i konwerterem DICOM należy skonfigurować za pomocą nazwy Hostname (Host) i ustawić Port na stronie konfiguracji Images (Obrazy).</p>	TCP 2762
	<p>Konwerter DICOM wysyła dane obrazów (w postaci konwertowanego pliku SVS lub surowych danych DICOM) do systemu zarządzania obrazami i danymi (IDMS) na serwerze DSR. Dane wysyłane są z użyciem szyfrowania SMB3.</p> <p>Komunikację pomiędzy konwerterem DICOM i serwerem DSR należy skonfigurować za pomocą ustawień File Location (lokalizacji plików) na stronie Images (Obrazy).</p>	UDP 137, 138 TCP 139, 445
	<p>Obrazy można wysyłać do stacji obrazowania podłączonych do serwera DSR.</p>	80, 443
Dane konfiguracyjne skanera	<p>Skaner wywołuje serwer SAM DX DataServer, aby zażądać przeprowadzenie konfiguracji danych. Serwer SAM DX DataServer przesyła dane konfiguracyjne do skanera. Dane wysyłane są z użyciem szyfrowania TLS. Komunikacja pomiędzy skanerem i serwerem SAM DX DataServer konfigurowana jest na skanerze.</p>	44386
	<p>Serwer SAM DX DataServer przechowuje dane konfiguracji w bazie danych serwera SQL na serwerze SAM DX.</p>	
	<p>Serwer SAM DX DataServer wyświetla dane konfiguracji poprzez stronę sieci Web serwera SAM DX.</p>	
Synchronizacja czasu	<p>Synchronizacja zegara pomiędzy serwerem SAM DX i wieloma skanerami utrzymywana jest za pomocą sieciowego protokołu czasu.</p>	UDP 123
Metadane obrazu	<p>Skaner wysyła metadane obrazów do serwera SAM DX DataServer. Dane wysyłane są z użyciem szyfrowania TLS. Komunikacja pomiędzy skanerem i serwerem SAM DX DataServer konfigurowana jest na skanerze.</p>	44386
	<p>Serwer SAM DX DataServer wysyła metadane obrazów do systemu IDMS, znajdującego się na serwerze DSR. Dane wysyłane są z użyciem szyfrowania TLS.</p> <p>Komunikację pomiędzy serwerem SAM DX DataServer i skanerem należy skonfigurować za pomocą nazwy hosta i ustawień portu na stronie serwera DSR.</p>	
Wysyłanie komunikatów i dane zdarzeń	<p>Skaner wysyła dziennika i dane zdarzeń do serwera Mirth Connect Server. Nie przesyłane są żadne dane wrażliwe.</p> <p>Komunikację pomiędzy skanerem i serwerem Mirth Connect Server należy skonfigurować na stronie konfiguracji Event Handling (obsługa zdarzeń).</p>	6662, 6663
	<p>Serwer Mirth Connect Server kopiuje krytyczne dane o zdarzeniach i błędach do serwera SAM DX DataServer, a następnie serwer SAM DX DataServer wysyła te dane do bazy danych SQL. Te dane raportowane są za pośrednictwem dzienników zdarzeń serwera SAM DX.</p>	
	<p>Serwer SAM DX DataServer wyświetla dane zdarzeń poprzez stronę sieci Web serwera SAM DX.</p>	
	<p>Serwer Mirth Connect Server przetwarza dane dziennika i dołącza dziennik zdarzeń, który znajduje się w systemie plików. Komunikacja pomiędzy serwerem Mirth i dziennikiem zdarzeń konfigurowana jest w konfiguracji aplikacji serwera Mirth. Nie jest dostępna poprzez aplikację SAM DX.</p>	

Punkt „Scanner Configuration Settings (Ustawienia konfiguracji skanera)” na stronie 23 dostarcza informacji o tym, w jaki sposób należy skonfigurować różne połączenia pomiędzy komponentami i usługami poprzez interfejs SAM DX.

3

Konfiguracja skanera Aperio GT 450 DX

Niniejszy rozdział zawiera informacje niezbędne do zmiany ustawień skanera, informacji systemowych lub konfiguracji. Konfiguracja skanera określa, w jaki sposób skaner komunikuje się z aplikacją SAM DX, i w jaki sposób aplikacja SAM DX komunikuje się z różnymi elementami w sieci, w tym z serwerem IDMS, konwerterem obrazów DICOM i innymi. Rozdział zawiera również procedury przypisywania kodów PIN dostępu do skanerów.

Instrukcje ogólne

Jedynie użytkownik z przypisaną rolą Lab Admin (Administrator laboratorium) mogą wprowadzać zmiany w konfiguracji. Operators (Operatorzy) mogą przeglądać ustawienia konfiguracji, ale nie mogą ich zmieniać.



Niektóre z ustawień konfiguracji określają sposób, w jaki skaner komunikuje się z SAM DX, np. Mac address (adres MAC) czy nazwa Hostname (Host). Serial Number (Numer seryjny) identyfikuje dany skaner. Ustawienia Calibration (Kalibracja) określają sposób działania skanera. Te ustawienia mogą być zmieniane wyłącznie przez personel działu pomocy technicznej firmy Leica i są wyświetlane w zaciemionych polach.

Obecne są trzy zestawy parametrów konfiguracji skanera:

- ▶ *Podstawowe ustawienia skanera*, takie jak adres sieci, nazwa i język wyświetlania
- ▶ *Informacje dotyczące systemu skanera (System Information)*, takie jak ogólne informacje i szczegółowe ustawienia skanera i kamery
- ▶ *Ustawienia Configuration (Konfiguracja) skanera*, takie jak ustawienia komunikacji dla konwertera obrazów DICOM i serwera DSR, zarządzania zdarzeniami, strefy czasowej i zarządzania kodami PIN

Niniejszy rozdział omawia każdy z zestawów parametrów.

Podstawowe ustawienia skanera

Edit Scanner

MAC Address
ac:1f:6b:27:da:55

Hostname
ScanAdmin

Name
Scanner Lab 1

Model
Aperio GT 450 DX


Serial Number
12008

Hardware Version
1.0.1

Language
English

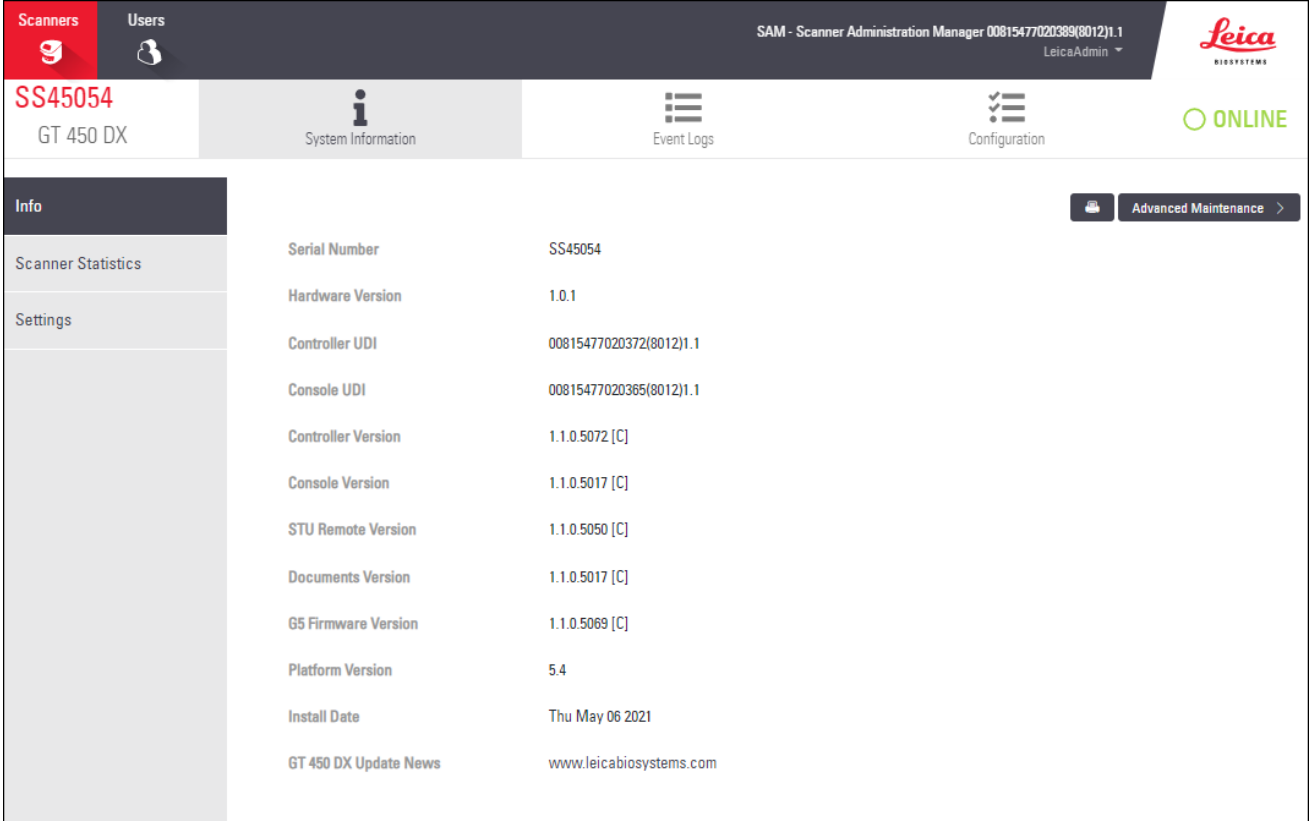
Save Cancel

Aby wyświetlić okno dialogowe Edit Scanner (Edytuj skaner):

1. Należy upewnić się, że ikona **Scanners** (Skanery) na banerze jest zaznaczona, a strona pokazuje listę skanerów. W razie konieczności kliknąć ikonę **Scanners** (Skanery), aby wyświetlić listę.
2. Najechać kursorem na nazwę skanera, tak aby ukazał się symbol edytowania , a następnie kliknąć nazwę skanera.
3. Dostosować dostępne ustawienia w miarę potrzeb:
 - ▶ Wprowadzić przyjazną nazwę (Friendly Name), aby zidentyfikować skaner dla placówki. (Przyjazna nazwa ukazywana jest na stronie głównej).
 - ▶ Jeśli użytkownik chce, może wybrać nowy język dla komunikatów panelu sterowania skanowania.
 - ▶ Dodatkowe informacje o każdej opcji znajdują się w punkcie „Załącznik B: Zestawienie ustawień skanera i opcji konfiguracji” na stronie 43.
4. Kliknąć **Save** (Zapisz), aby zapisać zmiany.

Jeśli ustawiany jest nowy skaner lub aby zmienić sposób komunikacji skanera z innymi serwerami w sieci, należy postępować według punktu „Scanner Configuration Settings (Ustawienia konfiguracji skanera)” na stronie 23.

Scanner System Information: Info Page (Informacje o systemie skanera: Strona informacji)



The screenshot shows the SAM - Scanner Administration Manager interface. The top navigation bar includes 'Scanners' and 'Users' tabs, the SAM title with a user ID, and the Leica Biosystems logo. The main content area is titled 'System Information' and displays details for scanner 'SS45054 GT 450 DX'. A sidebar on the left contains 'Info', 'Scanner Statistics', and 'Settings' sections. A table lists various system parameters and their values.

Serial Number	SS45054
Hardware Version	1.0.1
Controller UDI	00815477020372(8012)1.1
Console UDI	00815477020365(8012)1.1
Controller Version	1.1.0.5072 [C]
Console Version	1.1.0.5017 [C]
STU Remote Version	1.1.0.5050 [C]
Documents Version	1.1.0.5017 [C]
G5 Firmware Version	1.1.0.5069 [C]
Platform Version	5.4
Install Date	Thu May 06 2021
GT 450 DX Update News	www.leicabiosystems.com

Aby wyświetlić System Information Info (strona informacji o systemie):

1. Należy upewnić się, że ikona **Scanners** (Skanery) na banerze jest zaznaczona, a strona pokazuje listę skanerów. W razie konieczności kliknąć ikonę **Scanners** (Skanery), aby wyświetlić listę.
2. Kliknąć ikonę **System Information** (Informacje o systemie) po prawej stronie od skanera, który ma zostać sprawdzony.
3. Kliknąć **Info** na menu bocznym.

Sprawdzić ustawienia skanera na System Information Info (strona informacji o systemie). (Na tej stronie nie można wprowadzać zmian).

Wersje oprogramowania układowego i sprzętu są aktualizowane automatycznie po tym, jak SAM DX nawiąże komunikację ze skanerem.

Scanner System Information: Settings Page (Informacje o systemie skanera: Strona ustawień)

The screenshot shows the SAM - Scanner Administration Manager interface. The top navigation bar includes 'Scanners' and 'Users' tabs, and a user profile icon. The main header displays 'SCANNER LAB 1 Aperio GT 450 DX' and navigation icons for 'System Information', 'Event Logs', and 'Configuration'. A status indicator shows 'ONLINE'. The left sidebar lists configuration categories: 'Info', 'Scanner Statistics', 'Settings', 'Scanner Config', 'Camera Config', 'Scanner Additional Config', 'Focus Algorithm Config', 'RT Camera Config', 'RT Focus Config', 'Tissue Finder Config', 'Motion Config', 'Autoloader Config', and 'Debug Options'. The main content area is titled 'Scanner Config' and contains several input fields for macrofocus parameters: 'MACROFOCUS START' (11.75185), 'MACROFOCUS END' (10.75185), 'MACROFOCUS RESOLUTION' (0.000125), 'MACROFOCUS RAMPODIST' (0.1), 'MACROFOCUS POS OFFSET' (0), 'MACROFOCUS SNAP CHECK ENABLED' (a toggle switch that is currently turned on), and 'MACROFOCUS SNAP CHECK THRESHOLD' (350).

Strona System Information Settings (ustawienia informacji o systemie) wyświetla ustawienia kamery, skanera, algorytmu ogniska, ruchu i automatycznej ładowarki. (Na ilustracji powyżej widać jedynie niektóre spośród dostępnych ustawień). Większość ustawień lub wszystkie ustawienia na tej stronie zostaną skonfigurowane przez przedstawiciela firmy Leica Biosystems podczas instalacji skanera. Jednakże użytkownik może zostać poproszony o sprawdzenie ustawień podczas procedury rozwiązywania problemów.

W razie konieczności wprowadzenia zmian użytkownik otrzyma instrukcje od przedstawiciela działu pomocy technicznej firmy Leica Biosystems. Nie wolno zmieniać tych ustawień, chyba że na polecenie przedstawiciela działu pomocy technicznej firmy Leica Biosystems.

Aby skorzystać ze strony System Information Settings (ustawienia informacji o systemie) lub edytować ustawienia:

1. Należy upewnić się, że ikona **Scanners** (Skanery) na banerze jest zaznaczona, a strona pokazuje listę skanerów.
2. Kliknąć ikonę **System Information** (Informacje o systemie) po prawej stronie od skanera, który ma zostać sprawdzony.
3. Kliknąć **Settings** (Ustawienia) na menu bocznym.
4. Użyć paska przewijania, aby wyświetlić listę dostępnych ustawień.

Scanner Configuration Settings (Ustawienia konfiguracji skanera)

The screenshot displays the SAM web interface for configuring the DICOM image host. The top navigation bar includes 'Scanners' and 'Users' tabs, the SAM version (v1.8.1-prod.600b), and the Leica Biosystems logo. The main header shows 'PATHLAB 1 Aperio GT 450 DX' and navigation icons for System Information, Event Logs, and Configuration. The left sidebar lists various configuration categories, with 'Images' selected. The main panel shows the 'Configure settings for the DICOM image host' section with an 'Edit' button. The settings include:

- SCAN SCALE FACTOR: 1
- HOSTNAME: ScannerAdmin
- PORT: 2762
- TITLE: SVS_STORE_SCP
- FILE LOCATION: \\uscavs-eng-fs1\eng-share\Image_Quality\ss12011\RMA_TS
- IMAGE FILENAME FORMAT: (empty field with help icon)
- BARCODE VALUE IDENTIFIER: (empty field with help icon)
- BARCODE VALUE MODIFIER: (empty field with help icon)
- BARCODE VALUE SUBSTITUTION FORMAT: (empty field with help icon)
- REGULAR BARCODE ID: (toggle switch)

Ustawienia na tych stronach zostaną skonfigurowane przez przedstawiciela firmy Leica Biosystems podczas instalacji skanera. Jednakże użytkownik może zostać poproszony o sprawdzenie ustawień podczas procedury rozwiązywania problemów. Użytkownik być może będzie musiał zmodyfikować te ustawienia, jeśli w sieci zajdą zmiany, wpływające na co najmniej jedno z ustawień komunikacji. Jedynie użytkownik z przypisaną rolą Lab Admin (Administrator laboratorium) mogą wprowadzać zmiany w konfiguracji.

Dostępnych jest kilka stron Configuration (Konfiguracja), po jednej dla Images (Obrazy) (konwerter DICOM), DSR, Event handling (Zarządzanie zdarzeniami), PIN Management (Zarządzanie kodami PIN) i ustawienia Time Zone (Strefa czasowa).

- ▶ Ustawienia **Images** (Obrazy) kontrolują komunikację z serwerem, który jest hostem dla konwertera DICOM, jak również określają miejsce zapisu przekształconych danych obrazów w formacie SVS. Można również konfigurować inne pozycje. Zobacz „Strona obrazów” na stronie 25.
- ▶ Ustawienia **DSR** (Digital Slide Repository) kontrolują komunikację z systemem przechowywania obrazów, lub DSR, w którym przechowywane są metadane obrazów.

- ▶ Ustawienia **Event Handling** (Obsługa zdarzeń) kontrolują komunikację z serwerem, na którym przetwarzane są komunikaty skanera i zdarzenia (Mirth), Informacje dotyczące dzienników zdarzeń znajdują się w punkcie „*Obsługa dziennika zdarzeń*” na stronie 32.
- ▶ Ustawienia **PIN Management** (Zarządzanie kodami PIN) umożliwiają tworzenie jednego kodu lub większej ilości kodów PIN, zabezpieczających dostęp do skanera. Zobacz „*Zarządzanie kodami PIN*” na stronie 27, aby uzyskać dodatkowe informacje.

Aby skorzystać ze stron konfiguracji, aby wyświetlać lub edytować ustawienia:

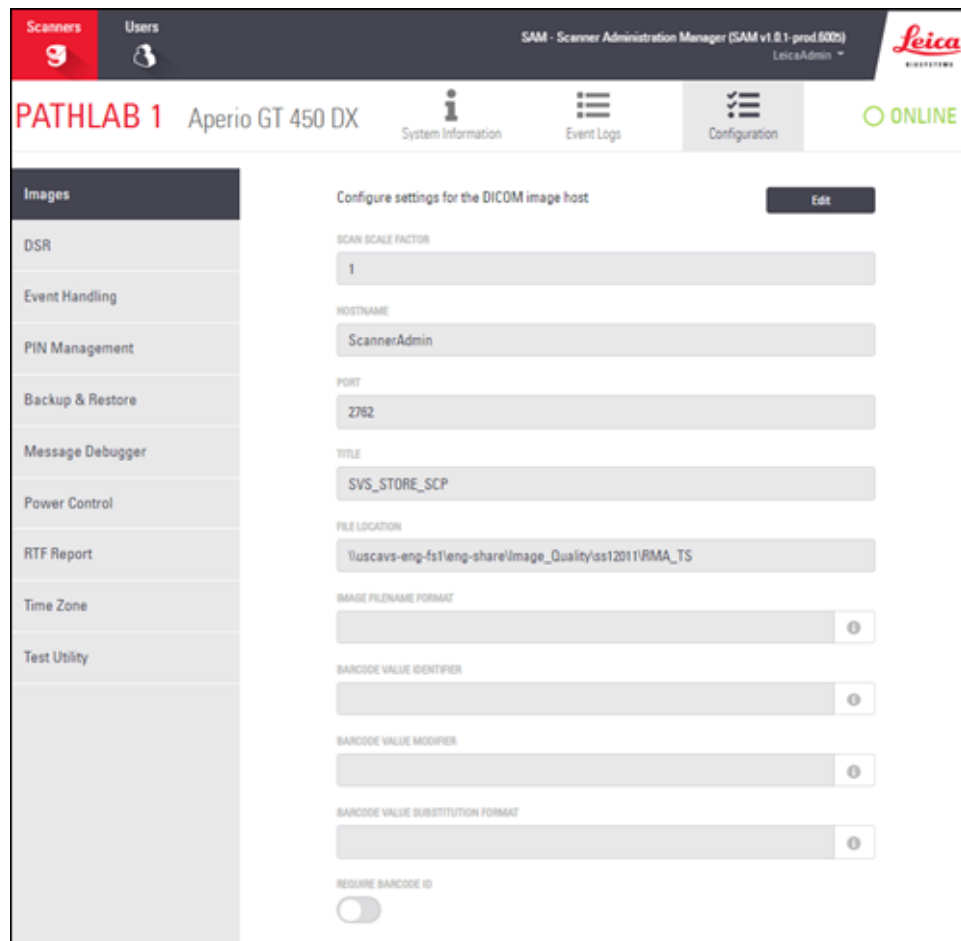
1. Należy upewnić się, że ikona **Scanners** (Skanery) na banerze jest zaznaczona, a strona pokazuje listę skanerów.
2. Kliknąć ikonę **Configuration** (Konfiguracja) po prawej stronie skanera, który ma zostać skonfigurowany. Wyświetli się strona konfiguracyjna Images (Obrazy).
3. Należy wprowadzić ustawienia konfiguracji dla obrazów (DICOM), DSR, obsługi zdarzeń, zarządzania kodami PIN lub strefy czasowej.
 - ▶ Kliknąć **Images** (Obrazy), **DSR**, **Event Handling** (Obsługa zdarzeń), **PIN Management** (Zarządzanie kodami PIN) lub **Time Zone** (Strefa czasowa) na bocznym pasku menu.
 - ▶ Kliknąć **Edit** (Edytuj), aby dokonać zmian na właściwej stronie. Należy mieć na uwadze, że nie można zmieniać ustawień w zaciemnionych polach.

Informacje dotyczące dodawania, usuwania lub modyfikowania kodów PIN lub zmiany limitów czasów znajdują się w punkcie „*Zarządzanie kodami PIN*” na stronie 27.

4. Jeśli dokonano zmian, należy kliknąć **Save** (Zapisz), aby zapisać zmiany i powrócić do trybu wyświetlania.

Dodatkowe informacje o każdej opcji znajdują się tutaj: „*Załącznik B: Zestawienie ustawień skanera i opcji konfiguracji*” na stronie 43.

Strona obrazów



Strona **Images** (Obrazy) zawiera ustawienia dla:

- ▶ Miejsca wysyłania zeskanowanych obrazów (wraz z nazwą serwera i lokalizacją pliku).
- ▶ Należy mieć na uwadze, że pola Title (Tytuł) i Scan Scale Factor (Współczynnik skalowania skanu) są przeznaczone do użytku wewnętrznego, Nie należy ich zmieniać, chyba że na polecenie pracownika działu pomocy technicznej firmy Leica Biosystems.
- ▶ Format nazwy pliku obrazu (patrz poniżej).
- ▶ Zarządzanie kodami kreskowymi (patrz poniżej).

Administrator laboratorium może kliknąć przycisk **Edit** (Edytuj), aby zmodyfikować ustawienia na tej stronie.

Format nazwy pliku obrazu

Domyślnie nazwa pliku zeskanowanego obrazu rozpoczyna się od numerycznego identyfikatora obrazu, po którym znajduje się podkreślenie i sześciocyfrowy kod, i wieńczy ją rozszerzenie pliku, wskazujące jego format.

Można wprowadzić własny tekst na początku tego pola, a następnie użyć dowolnego z tych słów kluczowych w dowolnej kolejności. Słowa kluczowe muszą być zapisane wielkimi literami i otoczone symbolami { }. Zalecamy oddzielanie słów kluczowych podkreśleniami, aby zwiększyć ich czytelność.

- ▶ **BARCODEID** – Identyfikator wartości kodu kreskowego (patrz następna sekcja)
- ▶ **RACK** – Numer koszyka
- ▶ **SLIDE** – Pozycja szkiełka w koszyku
- ▶ **IMAGEID** – Unikalny identyfikator obrazu

Na przykład, aby zidentyfikować wszystkie zeskanowane obrazy z tego skanera jako pochodzące ze skanera A, a ponadto wskazać koszyk i pozycję, z których szkiełko pochodzi, można stworzyć następujący format nazwy pliku obrazu:

SkanerA_{RACK}_{SLIDE}

Nazwa pliku będzie rozpoczynała się od tekstu „SkanerA”, po którym podany będzie numer koszyka i pozycja szkiełka w koszyku. Po tej nazwie znajdować się będzie podkreślenie, sześciocyfrowy kod i rozszerzenie pliku. Na przykład:

SkanerA_5_2_210164.SVS

Zarządzanie kodami kreskowymi

Kod kreskowy jest ciągiem tekstowym, zapisanym w pliku zeskanowanego obrazu, i może być wyświetlany w systemie zarządzania cyfrowymi szkiełkami.

W zależności od procedur stosowanych w danej instytucji na etykiecie szkiełka może znajdować się więcej niż jeden kod kreskowy. W takim przypadku konieczne będzie wskazanie kodu kreskowego, który ma być powiązany z zeskanowanym obrazem i wyświetlany w systemie zarządzania eSlide.

Aby to zrobić, należy wprowadzić ciąg w formacie regularnego wyrażenia w polu **Barcode Value Identifier** (Identyfikator wartości kodu kreskowego).

(Wyrażenie regularne, regex lub regexp, jest sekwencją znaków, definiujących wzór wyszukiwania. Na przykład: `\d{6}` określa, że używany będzie kod kreskowy z sześcioma cyframi w wierszu. Jeśli użytkownik nie jest zaznajomiony z wyrażeniami regularnymi, powinien skontaktować się z działem pomocy technicznej firmy Leica Biosystems).

Niektóre instytucje uwzględniają znaki kontrolne (niedrukowalne) w ich kodach kreskowych. Aby przefiltrować lub zastąpić te znaki, należy wprowadzić znaki, które mają zostać zmodyfikowane w formacie regularnego wyrażenia w polu **Barcode Value Modifier** (Modyfikator wartości kodu kreskowego). Na przykład: `[\x00-\x1f\x7f]` określa, że wszystkie niedrukowalne znaki zostaną zmodyfikowane.

Jeśli użytkownik chce podmienić niedrukowalne znaki zgodnie z wartością w polu **Barcode Value Modifier** (Modyfikator wartości kodu kreskowego), powinien wprowadzić tę wartość w polu **Barcode Value Substitution Format** (Format zamiany wartości kodu kreskowego). Na przykład: wartość „?” w połączeniu z wartością `[\x00-\x1f\x7f]` w polu **Barcode Value Modifier** (Modyfikator wartości kodu kreskowego) zamieni wszystkie niedrukowalne znaki ze znakiem zapytania „?”. Należy zostawić tę wartość pustą, aby usunąć znaki zgodne ze znakami w polu **Barcode Value Modifier** (Modyfikator wartości kodu kreskowego).

Jeśli procedury wymagają, aby każdy zeskanowany obraz był zapisywany z kodem kreskowym, należy przesunąć przycisk suwaka **Require Barcode ID** (Wymagaj identyfikatora kodu kreskowego) w prawo. Po aktywowaniu tej opcji skaner będzie pomijał szkiełka, które nie zawierają kodu kreskowego lub w przypadku których skaner nie był w stanie odczytać kodu kreskowego.

Funkcja omówiona w tej sekcji umożliwia wprowadzanie bardziej zaawansowanych modyfikacji kodów kreskowych. Jeśli potrzebna jest dodatkowa kontrola nad ciągiem kodu kreskowego, zwracającym do skanera Aperio GT 450 DX, należy skontaktować się z działem pomocy technicznej firmy Leica Biosystems.

Zarządzanie kodami PIN

Kody PIN kontrolują dostęp do skanera. (Każdy operator musi wprowadzić kod PIN, aby odblokować skaner).

Każdy kod PIN jest powiązany z określonym użytkownikiem skanera. Gdy operator uzyskuje dostęp do skanera za pomocą kodu PIN, skaner rejestruje nazwę użytkownika, powiązaną z tym kodem PIN w wewnętrznym dzienniku skanera. (Sam kod PIN nie jest rejestrowany). Elementy sterujące skanera pozostają odblokowane tak długo, jak operator wykonuje czynności. Jeśli przez ustawiony czas nie będzie żadnej interakcji ze skanerem, skaner zablokuje się do momentu wprowadzenia prawidłowego kodu PIN przez operatora.

- ▶ Dla każdego skanera należy przypisać co najmniej jeden kod PIN, a kody PIN są specyficzne dla poszczególnych skanerów. Można przypisać kod PIN aplikacji SAM DX lub inne kody PIN do każdego skanera w systemie w zależności od procedur stosowanych w placówce.
- ▶ Kod PIN nie ogranicza funkcji, do których operator ma dostęp na skanerze.
- ▶ Podczas konfigurowania limit czasu logowania należy wybrać czas wygodny dla operatorów, ale nie powinien on być na tyle długi, aby umożliwić użytkowanie skanera przez nieupoważnione osoby w wyniku pozostawienia go bez nadzoru.

Konfigurowanie kodu PIN i Timeout (Limit czasu)

Use this page to manage the list of valid PINs and adjust the PIN timeout for the scanner.

Console PIN Timeout (minutes)

PIN	LOGIN NAME	DESCRIPTION	TASKS
32116	BEwards	Senior Histotech, Lab2	
72451	LeeAlvarez	Histotech I, Lab 1	
00000	Operator		
12333	ScanAdmin		

1. Należy upewnić się, że ikona **Scanners** (Skanery) na banerze jest zaznaczona, a strona pokazuje listę skanerów.
2. Kliknąć ikonę **Configuration** (Konfiguracja) po prawej stronie skanera.
3. Kliknąć **PIN Management** (Zarządzanie kodami PIN) na menu bocznym.

4. Wprowadzić wartość (w minutach) w polu **Console PIN Timeout** (Limit czasu dla kodu PIN konsoli). Skaner zablokuje się automatycznie po upływie tego okresu nieaktywności.
5. Kliknąć **New PIN+** (Nowy PIN+), aby dodać nowy kod PIN. Pojawi się ekran New PIN (Nowy PIN).

- ▶ Wprowadzić kod PIN w polu kodu PIN (pięć cyfr). Kody PIN mogą zawierać wyłącznie cyfry – nie mogą zawierać znaków alfabetycznych ani specjalnych.
- ▶ Z listy rozwijanej Login Name (Nazwa loginu) należy wybrać użytkownika. Lista ta pokazuje wyłącznie użytkowników, którzy nie mają kodu PIN. (Informacje dotyczące dodawania użytkowników znajdują się tutaj: „Rozdział 5: Zarządzanie użytkownikami” na stronie 33.)
- ▶ Opcjonalnie można dodać Description (Opis), aby zidentyfikować użytkownika, który będzie korzystał z tego kodu PIN.
- ▶ Kliknąć **Save** (Zapisz), aby powrócić do listy kodów PIN.

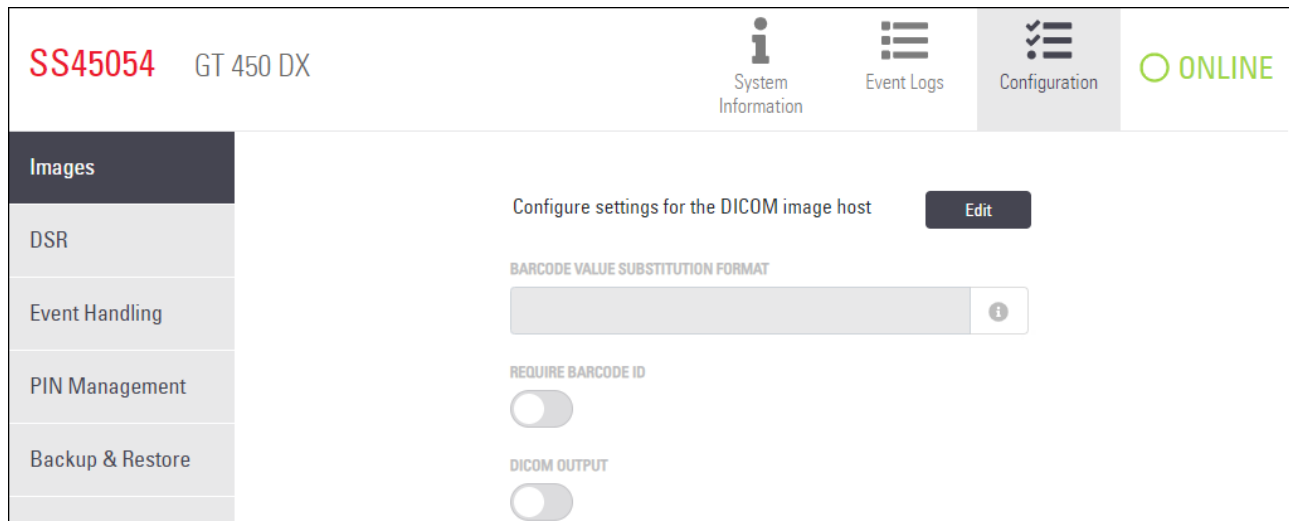
Aktywowanie wyjścia obrazów DICOM

Skaner Aperio GT 450 DX umożliwia tworzenie plików obrazów w formacie SVS lub DICOM. (Domyślnym formatem plików obrazów jest .SVS).

Można skorzystać z SAM DX, aby aktywować format DICOM dla poszczególnych skanerów.

i Zanim możliwe będzie aktywowanie tworzenia obrazów DICOM, środowisko informatyczne musi spełniać wymagania wymienione w **Deklaracji zgodności z DICOM firmy Aperio**. Ponadto przedstawiciel działu pomocy technicznej firmy Leica Biosystems musi zalogować się do aplikacji SAM DX jako administrator Leica i włączyć **Optional Features** (Opcjonalne funkcje) skanera, aby umożliwić konfigurację DICOM.

1. Należy zalogować się do aplikacji SAM DX jako administrator, przejść do głównej strony aplikacji SAM DX i kliknąć **Configuration** (Konfiguracja) obok skanera, dla którego ustawiony ma być format DICOM.
2. Kliknąć **Images** (Obrazy) na lewym panelu.



3. Kliknąć przycisk **Edit** (Edytuj) obok **Configure settings for DICOM image host** (Konfiguruj ustawienia dla hosta obrazów DICOM).
4. Przesunąć przycisk **DICOM Output** (Wyjście DICOM) w prawo. [Przycisk **Edit** (Edytuj) zamieni się w przycisk **Save** (Zapisz)].
5. Kliknąć przycisk **Save** (Zapisz).

Podczas używania skanera, który został skonfigurowany tak, aby tworzył obrazy w formacie DICOM, na górze strony Console (Konsola) będzie znajdować się komunikat „(DICOM)“:

Aperio GT 450 DX (DICOM)

4

Wyświetlanie informacji o systemie

Niniejszy rozdział opisuje, jak należy wyświetlać różne opcje konfiguracji i ustawień serwera SAM DX.

Wyświetlanie informacji o skanerze i ustawień

Aby wyświetlić ustawienia skanera i systemu, należy postępować zgodnie z instrukcjami, podanymi w tabeli poniżej.

W wielu przypadkach modyfikowanie tych ustawień jest niemożliwe, ale dział pomocy technicznej firmy Leica Biosystems może poprosić o podanie informacji w trakcie rozwiązywania problemów lub konserwacji. Niektóre ustawienia widoczne są wyłącznie dla użytkowników z rolą Lab Admin (Administrator laboratorium).

Aby wyświetlić:	Należy:
Mac Address (Adres Mac)	Wybrać skaner na ekranie głównym, aby wyświetlić okno dialogowe Edit Scanner (Edytuj skaner)
Scanner Hostname (Nazwa hosta skanera)	
Scanner Friendly Name (Nazwa przyjazna skanera)	
Scanner Model (Model skanera)	
Scanner Language (Język skanera)	
Scanner Serial Number (Numer seryjny skanera)	Wybrać skaner na ekranie głównym, aby wyświetlić okno dialogowe Edit Scanner (Edytuj skaner), lub Kliknąć System Information (Informacje o systemie) dla skanera, a następnie kliknąć Info na menu bocznym
Scanner Firmware Version (Wersja oprogramowania układowego skanera)	Kliknąć System Information (Informacje o systemie) dla skanera, a następnie kliknąć Info na menu bocznym
Scanner Hardware Version (Wersja sprzętu skanera)	
Scanner Installation Date (Data instalacji skanera)	
DICOM Server Settings (Ustawienia serwera DICOM)	Kliknąć Configuration (Konfiguracja) dla skanera, a następnie kliknąć Images (Obrazy) na menu bocznym
DSR Server Settings (Ustawienia serwera DSR)	Kliknąć Configuration (Konfiguracja) dla skanera, a następnie kliknąć DSR na menu bocznym


Aby wyświetlić:	Należy:
Event Handling (Mirth server) Settings (Ustawienia obsługi zdarzeń (serwer Mirth))	Kliknąć Configuration (Konfiguracja) dla skanera, a następnie kliknąć Event Handling (Obsługa zdarzeń) na menu bocznym
Camera Configuration Settings (Ustawienia konfiguracji kamery)	Kliknąć System Information (Informacje o systemie) dla skanera, a następnie kliknąć Settings (Ustawienia) na menu bocznym
Scanner Additional Config Settings (Dodatkowe ustawienia konfiguracji skanera)	
Focus Algorithm Config Settings (Ustawienia konfiguracji algorytmu ogniska)	
Motion Config XML File (Plik konfiguracji ruchu XML)	
Autoloader Config XML File (Plik konfiguracji automatycznej podawarki XML)	
List of Users (Lista użytkowników)	Kliknąć ikonę Users (Użytkownicy) na górnym banerze
List of PINs (Lista kodów PIN)	Kliknąć Configuration (Konfiguracja) dla skanera, a następnie kliknąć PIN Management (Zarządzanie kodem PIN) na menu bocznym

Wyświetlanie statystyk dotyczących skanera

Konsola SAM DX może wyświetlać te same statystyki skanera, jak te, które są dostępne na wyświetlaczu panelu sterującego skanera.

Zarówno użytkownicy z rolą Operator jak i Lab Admin (Administrator laboratorium) mogą wyświetlać statystyki.

Aby wyświetlić statystykę skanera:

1. Należy upewnić się, że ikona Scanners (Skanery) na banerze jest zaznaczona, a strona pokazuje listę skanerów.
2. Kliknąć ikonę **System Information** (Informacje o systemie) po prawej stronie skanera.
3. Kliknąć **Scanner Statistics** (Statystyki skanera) na menu bocznym.
4. Wybrać okres wyświetlania spośród wyborów, znajdujących się nad siatką.
5. Kliknąć , aby wydrukować statystyki. Należy użyć okna dialogowego drukarki, aby określić drukarkę i inne opcje drukowania.

Obsługa dziennika zdarzeń

Aby wyświetlić dziennik zdarzeń:

1. Należy upewnić się, że ikona Scanners (Skanery) na banerze jest zaznaczona, a strona pokazuje listę skanerów.
2. Kliknąć ikonę **Event Logs** (Dzienniki zdarzeń) po prawej stronie skanera.
Ekran wyświetli wszystkie błędy i zdarzenia od ostatniego wyczyszczenia ekranu. Na tym ekranie należy wykonać następujące czynności:

- ▶ Kliknąć przycisk **Download All Logs** (Pobierz wszystkie dzienniki), aby zapisać plik .zip w folderze Downloads (Pobrane) serwera SAM DX.



*Aby możliwe było użycie przycisku **Download All Logs** (Pobierz wszystkie dzienniki), stacja robocza musi być podłączona do sieci LAN instytucji z dostępem do serwera SAM DX; aby skorzystać z tej funkcji stacja nie może uzyskać dostępu do serwera SAM DX zdalnie spoza sieci LAN.*

- ▶ Kliknąć **Clear Current Screen** (Wyczyść bieżący ekran), aby usunąć wszystkie wpisy z ekranu. Należy mieć na uwadze, że to nie spowoduje usunięcia wpisów w dzienniku.

Tworzenie kopii zapasowej plików dziennika

Zalecamy wykonanie kopii zapasowej plików dziennika skanera, pobranych z serwera SAM DX, i zapisanie ich w innym miejscu. Zalecamy również stworzenie kopii zapasowych dzienników zdarzeń systemu Windows na serwerze SAM DX i zapisanie ich w innym miejscu.

Alerty logowania

Plik dziennika konsoli zawiera zdarzenia związane z logowaniem użytkownika, takie jak pomyślne logowania za pomocą nazw użytkowników. Zawiera on również ostrzeżenia o nieudanych próbach logowania.

Dziennik może również pokazać komunikat „Possible Intrusion Detected” (Wykryto potencjalną próbę włamania) w przypadku rozbieżności dotyczących logowania, mających miejsce podczas uzyskiwania dostępu do skanera zdalnie poprzez SSH.

5

Zarządzanie użytkownikami

Niniejszy rozdział zawiera informacje dotyczące konfigurowania kont użytkowników dla aplikacji SAM DX.

Aby móc zalogować się do SAM DX, by wyświetlić lub edytować ustawienia systemu lub skanera, użytkownik musi mieć konto. Konta użytkowników SAM DX mają dostęp do wszystkich skanerów na serwerze SAM DX.

Administrator tworzy konto dla każdego użytkownika i jednocześnie przypisuje im role. Rola użytkownika określa, co użytkownik może, a czego nie może robić w systemie.

Rozumienie roli

Istnieją trzy role użytkowników:

- ▶ Rola Operator
- ▶ Rola Lab Admin (Administrator laboratorium)
- ▶ Leica Support (Pomoc techniczna firmy Leica)

Rola	Opis
Rola Operator	<p>Jest to rola ogólnego zastosowania, odpowiednia dla większości użytkowników. Użytkownicy z rolą operatora mogą wyświetlić większość ustawień systemu i wykonać poniższe czynności:</p> <ul style="list-style-type: none">• Wyświetlić status każdego skanera• Wyświetlić informacje o systemie dla każdego skanera<ul style="list-style-type: none">• Uzyskać dostęp do strony Info (Informacje)• Uzyskać dostęp do strony Scanner Statistics (Statystyki skanera)• Uzyskać dostęp do strony Settings (Ustawienia)• Wyświetlić Event Log (Dziennik zdarzeń)• Zmienić swoje hasło <p>Operatorzy nie mogą wyświetlać ani zmieniać kody PIN, przypisane do skanera.</p> <p>Operatorzy nie mogą wyświetlić listy użytkowników ani zmieniać ustawień dla innych użytkowników</p>

Rola	Opis
Rola Lab Admin (Administrator laboratorium)	<p>Ta rola zapewnia zaawansowany dostęp administracyjny i jest odpowiednia dla użytkowników, którzy muszą dodawać konta użytkowników lub zarządzać nimi, lub wprowadzać zmiany w systemie. Dodatkowo do funkcji dostępnych dla operatorów, użytkownicy z rolą Administrator mogą wykonać poniższe czynności:</p> <ul style="list-style-type: none"> • Dodawać, modyfikować i usuwać inne konta użytkowników • Zmieniać hasła użytkowników • Wyświetlać System Information (Informacje o systemie) i edytować niektóre ustawienia • Edytować ustawienia Configuration (Konfiguracja): <ul style="list-style-type: none"> • Images (Obrazy) • DSR • Event Handling (Obsługa zdarzeń) • PIN Management (Zarządzanie kodami PIN)
Leica Support (Pomoc techniczna firmy Leica)	<p>Jest to chroniona rola, która nie może zostać przypisana użytkownikom. Ta rola (której nazwa to Leica Admin) nie może zostać usunięta z systemu.</p> <p>Używana jest przez przedstawicieli działu pomocy technicznej firmy Leica do rozwiązywania problemów, konserwacji i napraw, a także zapewnia możliwość dodawania skanerów do systemu i usuwania ich z niego.</p>

Zarządzanie użytkownikami

Jedynie użytkownicy z rolą Lab Admin (Administrator laboratorium) mogą wyświetlać lub modyfikować listę użytkowników bądź modyfikować istniejące konta użytkowników.

Dodawanie użytkownika

1. Wybrać **Users** (Użytkownicy) z górnej wstążki na stronie głównej.
2. Kliknąć **Add User** (Dodaj użytkownika) na dole strony z listą użytkowników.
3. Wprowadzić informacje dla nowego konta użytkownika:
 - ▶ Nazwa loginu (od 1 do 296 znaków, może zawierać litery, cyfry i znaki specjalne)
 - ▶ Pełna nazwa użytkownika
4. Wprowadzić początkowe hasło. Hasła mają następujące wymagania:
 - ▶ Co najmniej 10 znaków
 - ▶ Co najmniej jedną wielką literę i jedną małą literę
 - ▶ Co najmniej jedną cyfrę
 - ▶ Co najmniej jeden znak specjalny: ! @ # \$ % ^ * or _
 - ▶ Inne od poprzednich 5 haseł

5. Wybrać rolę: Lab Admin (Administrator laboratorium) lub Operator.
6. Kliknąć przycisk **Save** (Zapisz).

Edytowanie użytkownika

1. Wybrać **Users** (Użytkownicy) z górnej wstążki na stronie głównej.
2. Kliknąć **Edit** (Edytuj) obok nazwy użytkownika, która ma być edytowana.
3. Wprowadzić nowe informacje.
Należy mieć na uwadze, że nie można zmienić roli istniejącego konta użytkownika.
4. Kliknąć przycisk **Save** (Zapisz).

Usuwanie użytkownika

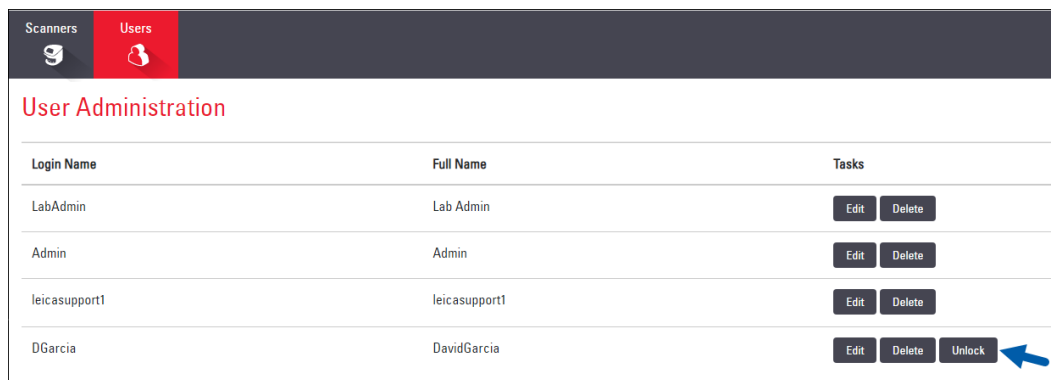
1. Wybrać **Users** (Użytkownicy) z górnej wstążki na stronie głównej.
2. Kliknąć **Delete** (Usuń) obok nazwy użytkownika, który ma zostać usunięty.
3. Potwierdzić zamiar usunięcia użytkownika lub kliknąć **Cancel** (Anuluj).

Odblokowanie konta użytkownika

Po trzech nieudanych próbach logowania do serwera SAM DX, aplikacja SAM DX zablokuje takiego użytkownika.

Użytkownik z rolą Lab Admin (Administrator laboratorium) może odblokowywać konta operatorów. (Użytkownik LeicaAdmin może odblokowywać wszystkie konta).

1. Wybrać **Users** (Użytkownicy) z górnej wstążki na stronie głównej.
2. Kliknąć **Unlock** (Odblokuj) obok nazwy użytkownika, który ma zostać odblokowany.



Login Name	Full Name	Tasks
LabAdmin	Lab Admin	Edit Delete
Admin	Admin	Edit Delete
leicasupport1	leicasupport1	Edit Delete
DGarcia	DavidGarcia	Edit Delete Unlock

Zmiana hasła użytkownika

Po pomyślnym logowaniu każdy użytkownik może zmienić swoje hasło:

1. Wybrać nazwę użytkownika, widoczną w prawym górnym obszarze strony głównej.
2. Kliknąć łącze **Change Password** (Zmień hasło).
3. Wprowadzić hasło. Wymagania dla haseł są następujące:
 - ▶ Co najmniej 10 znaków
 - ▶ Co najmniej jedną wielką literę i jedną małą literę
 - ▶ Co najmniej jedną cyfrę
 - ▶ Co najmniej jeden znak specjalny: ! @ # \$ % ^ * or _
 - ▶ Inne od poprzednich 5 haseł
4. Potwierdzić hasło, a następnie kliknąć **OK**.

6

Wytyczne dotyczące cyberbezpieczeństwa i sieci

Niniejszy rozdział omawia, w jaki sposób skaner Aperio GT 450 DX i aplikacja Aperio SAM DX chronią elektronicznie zabezpieczone informacje o zdrowiu (E PHI) i zapewniają ochronę przed zagrożeniami dla cyberbezpieczeństwa. Omawia również środki, jakie można podjąć, aby chronić serwer SAM DX w sieci. Niniejszy rozdział zawiera informacje dla administratorów sieci informatycznej, administratorów produktów firmy Aperio, a także użytkowników końcowych produktów firmy Aperio.



PRZESTROGA: Należy zapoznać się ze wszystkimi wytycznymi, zawartymi w niniejszym rozdziale, aby uzyskać informacje o ochronie skanera Aperio GT 450 DX i aplikacji Aperio SAM DX przed zagrożeniami dla cyberbezpieczeństwa.

Zalecenia zawarte w niniejszej sekcji dotyczą serwerów opartych na systemie Windows, które są hostami dla aplikacji SAM DX. Ustawienia bezpieczeństwa i sieciowe są konfigurowane poprzez system operacyjny Windows i jego narzędzia administracyjne. Treść niniejszej sekcji ma charakter wyłącznie informacyjny. Szczegółowe instrukcje znajdują się w dokumentacji systemu Windows.

W wielu przypadkach placówka może wymagać ustawień i konfiguracji bezpieczeństwa, które są bardziej rygorystyczne niż te wymienione tutaj. W takim przypadku należy stosować bardziej rygorystyczne wytyczne i wymagania, dyktowane przez placówkę.



Po zainstalowaniu produktu Aperio GT 450 DX przedstawiciel firmy Leica Biosystems przekaze działowi informatycznemu placówki informacje związane z cyberbezpieczeństwem, takie jak dane uwierzytelniające certyfikatu SSL, klucz szyfrowania dysku serwera SAM DX itp. Te informacje stają się własnością klienta i jego odpowiedzialnością jest ich ochrona.

Funkcje cyberbezpieczeństwa skanera Aperio GT 450 DX i aplikacji Aperio SAM DX

Funkcje cyberbezpieczeństwa zawarte w produkcie Aperio GT 450 DX chronią krytyczne funkcje, pomimo naruszenia cyberbezpieczeństwa. Tymi funkcjami są:

- ▶ Redukowanie wrażliwości cyberbezpieczeństwa, właściwe systemy operacyjne na VPU Aperio GT 450 DX i serwerze SAM DX zabezpieczone są za pomocą wzorców CIS (Center for Internet Security).
- ▶ Skaner Aperio GT 450 DX i serwer SAM DX nie są przeznaczone do przechowywania wrażliwych danych, a jedynie do eksportowania/przesyłania danych do podłączonych aplikacji na oddzielnych serwerach sieciowych. Połączenie pomiędzy skanerem Aperio GT 450 DX i serwerem SAM DX jest uwierzytelniane poprzez szyfrowane, bezpieczne połączenie SSL/TLS.

- ▶ Skaner Aperio GT 450 DX używa listy dopuszczeń/odrzuceń i zaleca się, aby serwer SAM DX również niej korzystał. To uniemożliwia pracę nieautoryzowanego oprogramowania na tych komponentach.
- ▶ Codzienne czynności konserwacyjne dla skanera Aperio GT 450 DX obejmują ponowne uruchomienie każdego dnia. (Szczegółowe informacje znajdują się w *Instrukcji obsługi Aperio GT 450 DX*). To odświeża oprogramowanie układowe.
- ▶ Plik Console.log skanera GT 450 DX zawiera zdarzenia związane z logowaniem wraz z nazwami użytkowników. Dziennik może również pokazać komunikat „Possible Intrusion Detected” (Wykryto potencjalną próbę włamania) w przypadku rozbieżności dotyczących logowania, mających miejsce podczas uzyskiwania dostępu do skanera zdalnie poprzez SSH. Szczegółowe informacje dotyczące plików dzienników znajdują się tutaj „*Obsługa dziennika zdarzeń*” na stronie 32.

Ochrona danych

Nieużywane dane chronione są poprzez szyfrowanie. Jednakże ze względu na ograniczenia systemu operacyjnego prywatne informacje o zdrowiu (Private Health Information, PHI) nie mogą być chronione w trakcie przesyłania. Firma Leica Biosystems zaleca, aby chronić dane w trakcie przesyłania za pomocą SSL z silnymi protokołami bezpieczeństwa, takimi jak szyfrowanie Transport Layer Security (TLS) lub szyfrowanie na poziomie sieci, np. tunelowanie IPsec lub SSH.

Fizyczne zabezpieczenia skanera Aperio GT 450 DX

- ▶ Skaner Aperio GT 450 DX należy chronić poprzez ograniczanie nieupoważnionego fizycznego dostępu do niego.

Ochrona serwera SAM DX

Poniższe sekcje zawierają zalecenia dotyczące ochrony serwera SAM DX.

Ochrona za pomocą hasła, loginu i konfiguracji użytkownika

- ▶ Zalecamy stosowanie następujących wymagań w zakresie złożoności hasła dla użytkowników logujących się do klienta sieciowego SAM DX:
 - Hasła muszą zawierać co najmniej 8 znaków, w tym:
 - Jedną wielką literę
 - Jedną cyfrę
 - Jedną małą literę
 - Jeden znak specjalny z poniższego zestawu: ! @ # \$ % ^ * _
 - Nie można ponownie użyć ostatnich pięciu haseł.
- ▶ Po trzech nieprawidłowych próbach logowania konto użytkownika jest blokowane. Użytkownik może skontaktować się z administratorem SAM DX, aby odblokować konto.
- ▶ Zalecamy skonfigurowanie stacji roboczych używanych do logowania do SAM DX w taki sposób, aby ekran limitu czasu wyświetlany był po 15 minutach nieaktywności i wymagał od użytkowników ponownego zalogowania po tym czasie.
- ▶ Ze względów bezpieczeństwa nie należy używać takich nazw użytkowników jak „Admin”, „Administrator” czy „Demo” przy dodawaniu użytkowników do SAM DX.

Fizyczne zabezpieczenia dla serwera SAM DX

- ▶ Należy chronić serwer SAM DX i stacje robocze klienta, używane do logowania do SAM DX, przed nieupoważnionym dostępem poprzez ograniczanie fizycznego dostępu do nich.
- ▶ Aby chronić serwer SAM DX przed złośliwym oprogramowaniem, należy zachować ostrożność podczas podłączania napędów USB i innych urządzeń wymiennych. Warto rozważyć wyłączenie portów USB, które nie są używane. Po podłączeniu dysku USB lub innego urządzenia wymiennego, należy przeskanować je za pomocą programu antywirusowego.

Zabezpieczenia administracyjne serwera SAM DX

- ▶ Należy skonfigurować zezwolenia dla użytkowników w taki sposób, aby umożliwić im dostęp jedynie do tych części systemów, które są dla nich niezbędne do wykonania pracy. W przypadku serwera SAM DX rolami użytkowników są „Operator” i „Lab Admin” (Administrator laboratorium), które mają różne uprawnienia.
- ▶ Należy chronić serwer SAM DX i stacje robocze klienta przed nieupoważnionym dostępem za pomocą standardowych technik informatycznych. Na przykład:
 - Zapory sieciowe – Zalecamy włączenie zapory sieciowej systemu Windows na stacjach roboczych klientów.
 - Zezwolić na listowanie, które jest narzędziem administracyjnym, które umożliwia pracę jedynie uwierzytelnionym programom, na serwerze SAM DX.
- ▶ Firma Leica Biosystems zaleca stosowanie standardu SQL (2019 lub nowszego) lub serwera SQL typu Enterprise, który oferuje funkcję szyfrowania bazy danych.
- ▶ Zachowywać normalną ostrożność przy konserwowaniu i korzystaniu z serwerów. Przerwanie połączeń sieciowych lub wyłączenie serwerów podczas przetwarzania danych (np. podczas analizy szkiełek cyfrowych lub generowania raportu z audytu) może spowodować utratę danych.
- ▶ Dział informatyczny placówki musi dbać o sprawność serwera poprzez wdrażanie poprawek bezpieczeństwa systemu Windows i Aperio oraz poprawek, które mogą być dostępne dla systemu.
- ▶ Należy wybrać serwer, który może zostać skonfigurowany pod kątem wykrywania prób uzyskania nieautoryzowanego dostępu i w taki sposób, aby automatycznie blokował konta używane do takich ataków, informując administratorów o takich zdarzeniach.
- ▶ Należy przestrzegać polityki bezpieczeństwa instytucji w zakresie ochrony danych przechowywanych w bazie danych.
- ▶ Zalecamy wdrożenie funkcji listowania na serwerze, tak aby możliwe było uruchomienie wyłącznie autoryzowanych aplikacji

Jeśli funkcja listowania nie jest używana, zdecydowanie zalecamy zainstalowanie oprogramowania antywirusowego na serwerze. Należy przeprowadzać skanowanie antywirusowe co najmniej raz na 30 dni.

Zalecamy również skonfigurowanie oprogramowania antywirusowego w taki sposób, aby nie obejmowało plików typu .SVS i DICOM, jak również magazynu plików z funkcją „skanowania przy dostępie”, ponieważ te pliki bywają bardzo duże i są często pozostają otwarte w trakcie skanowania i wyświetlania szkiełek cyfrowych przez użytkowników. Skany pod kątem wirusów można skonfigurować w taki sposób, aby przeprowadzane były poza godzinami szczytu, ponieważ w wysokim stopniu obciąża procesor i może zakłócać skanowanie.

- ▶ Należy okresowo tworzyć kopie zapasowe dysków twardych na serwerze.
- ▶ W przypadku połączenia sieciowego pomiędzy SAM DX i DSR zalecamy używanie serwera magazynu, który obsługuje protokół sieciowy SMB3, aby chronić przesyłane dane. Jeśli serwer DSR nie obsługuje protokołu SMB3 lub nowszego, należy wdrożyć środki ograniczające ryzyko, aby chronić dane w trakcie przesyłania.
- ▶ Zalecamy szyfrowanie treści dysków twardych serwera.
- ▶ Udziały plików na serwerze powinny być zabezpieczone przed nieautoryzowanym dostępem za pomocą ogólnie przyjętych praktyk informatycznych.
- ▶ Należy aktywować rejestrowanie zdarzeń w systemie Windows na serwerze, aby śledzić próby uzyskiwania dostępu przez użytkowników i zmiany w folderach danych, które zawierają informacje o pacjentach i obrazy. Należy również tworzyć kopie zapasowe plików dzienników i przechowywać je w innym miejscu. Zobacz „*Obsługa dziennika zdarzeń*” na stronie 32.

Korzystanie z gotowego, komercyjnie dostępnego oprogramowania

Podczas przeprowadzania ocen cyberbezpieczeństwa użytkownik może chcieć rozważyć, z jakich komponentów oprogramowania zewnętrznych producentów korzystać powinno oprogramowanie firmy Leica Biosystems. Firma Leica Biosystems utrzymuje listy wszystkich gotowych komercyjnych programów (OTS), używanych przez skaner Aperio GT 450 DX i serwer SAM DX. Aby uzyskać informacje na temat stosowanych OTS, należy skontaktować się z przedstawicielem działu sprzedaży lub działu obsługi klienta firmy Leica Biosystems i poprosić o zestawienie oprogramowania dla skanera Aperio GT 450 DX i serwera SAM DX.

Obsługa i poprawki cyberbezpieczeństwa

Należy mieć na uwadze, że pomoc techniczna i poprawki cyberbezpieczeństwa dla skanera Aperio GT 450 DX i serwera Aperio SAM DX mogą nie być dostępne po upływie żywotności produktu, określonej w *Podręczniku użytkownika skanera Aperio GT 450 DX*.

A

Rozwiązywanie problemów

Niniejszy załącznik zawiera przyczyny i rozwiązania problemów związanych z serwerem SAM DX i powiązаныmi komponentami. Zawiera również procedury rozwiązywania problemów, które można przeprowadzić jako administrator laboratoryjny urządzenia Aperio GT 450 DX. Ogólne informacje dotyczące rozwiązywania problemów dla operatora skanera znajdują się w *Podręczniku użytkownika skanera Aperio GT 450 DX*.

Rozwiązywanie problemów związanych z aplikacją Scanner Administration Manager DX (SAM DX)

Objawy	Przyczyna	Rozwiązanie
Komunikat o błędzie „Credentials are Invalid” („Dane uwierzytelniające są nieprawidłowe”) podczas logowania	Instancja usługi DataServer używana przez SAM SX nie działa	Należy ponownie uruchomić usługę DataServer na serwerze SAM DX. <i>Zobacz „Uruchomić ponownie DataServer” na stronie 42.</i>
	Nieprawidłowe dane uwierzytelniające	Sprawdzić, czy klawisz caps lock nie jest wciśnięty itp. Zweryfikować dane uwierzytelniające z Administratorem
Po aktualizacji nowe funkcje w interfejsie użytkownika SAM DX są niedostępne	Aplikacja jest buforowana w przeglądarce	Należy zamknąć SAM DX i wyczyścić pamięć podręczną przeglądarki
Skaner jest włączony i podłączony do SAM DX (pobiera jego ustawienia), ale SAM DX pokazuje, że skaner jest odłączony i nie raportuje żadnych danych statystycznych (liczby skanów itp.).	Mirth na serwerze SAM DX nie działa.	<i>Zobacz „Sprawdzić, czy Mirth działa” na stronie 42.</i>
	Porty nie są otwarte	Należy upewnić się, że port 6663 jest otwarty w zaporze sieciowej i jest dostępny dla skanera.

Objawy	Przyczyna	Rozwiązanie
Pliki dziennika skanera nie pojawiają się w folderze dzienników skanera	Mirth na serwerze SAM DX nie działa.	Zobacz „ <i>Uruchomić ponownie DataServer</i> ” poniżej.
	Folder wyjściowy dziennika jest skonfigurowany nieprawidłowo.	Sprawdź zakładkę Configuration Map (Mapa konfiguracji) w ustawieniach (AppLog_Dir).
	Błąd Mirth	Należy sprawdzić Mirth Dashboard pod kątem wszelkich błędów związanych z kanałem „ScannerAppLogWriter” i zapoznać się z dziennikiem błędów Mirth, aby uzyskać dodatkowe informacje.
	Porty nie są otwarte	Należy upewnić się, że port 6663 jest otwarty w zaporze sieciowej i jest dostępny dla skanera.
Interfejs użytkownika SAM DX jest niedostępny lub zwraca kod błędu przy próbie nawiązania połączenia	Błąd IIS	Należy upewnić się, że IIS i witryna działają i że porty, na których SAM DX jest dostępny, są otwarte w zaporze sieciowej.
	Błąd konfiguracji uwierzytelniania anonimowego w IIS	Sprawdzić konfigurację IIS. Zobacz „ <i>Błąd konfiguracji IIS</i> ” poniżej.

Uruchomić ponownie DataServer

Na serwerze należy przejść do menedżera usług i upewnić się, że usługa „ApDataService” działa. Jeśli usługa ta nie uruchomia się lub błąd się powtarza, należy sprawdzić dzienniki DataServer (zazwyczaj znajdują się w katalogu C:\Program Files (x86)\Aperio\DataServer\Logs).

Sprawdzić, czy Mirth działa

Na serwerze upewnić się, że serwer Mirth Connect działa. Jeśli działa, należy upewnić się, że ustawienia mapy konfiguracji ustawione są tak, że kierują do prawidłowego hosta DataServer (SAM DX_Host) i portu (SAM DX_Port) i używają prawidłowego połączenia SSL lub nie SSL (SAM DX UriSchema). Jeśli Dashboard (Pulpit) nawigacyjny w Mirth Connect zgłasza błędy na kanale „ScannerEventProcessor”, należy sprawdzić dzienniki błędów Mirth, aby uzyskać dodatkowe informacje. Jeśli DataServer nie pracuje, mogą pojawiać się błędy kanału Mirth. Należy upewnić się, że port 6663 jest otwarty w zaporze sieciowej i jest dostępny dla skanera.

Błąd konfiguracji IIS

Aby sprawdzić to ustawienie, należy otworzyć witrynę w IIS i przejść do ustawień Authentication (Uwierzytelnianie). Znaleźć i edytować pozycję Anonymous Authentication (Uwierzytelnianie anonimowe) i upewnić się, że ustawionym określonym użytkownikiem jest „IUSR” (bez hasła). Jeśli witryna jest uruchomiona i wszystkie ustawienia są prawidłowe, należy zapoznać się z dziennikami IIS, aby uzyskać dodatkowe informacje.

B

Zestawienie ustawień skanera i opcji konfiguracji

Niniejszy załącznik zawiera wykaz ustawień i opcji konfiguracji. Tabele te powinny pełnić funkcję list kontrolnych w trakcie gromadzenia informacji niezbędnych w celu dodania lub ponownego skonfigurowania skanera. Należy mieć na uwadze, że podczas instalacji większość z tych ustawień i opcji konfiguracji zostanie skonfigurowana przez przedstawiciela firmy Leica Biosystems.

Podstawowe informacje o skanerze

Lab Administrators (Administratorzy laboratorium) mogą wybrać nazwę skanera ze strony skanera, aby wyświetlić podstawowe ustawienia skanera. (Operatorzy mogą zobaczyć niektóre z ustawień na stronie System Information (Informacje o systemie)). Ani Lab Administrator (Administrator laboratorium), ani operatorzy nie mogą zmieniać żadnych ustawień wyświetlanych w szarych polach.

Ustawienie	Opis	Widok/Edycja	
		Administrator	Operator
Mac Address (Adres MAC)	Określane podczas instalacji	Widok	Brak
Hostname (Nazwa hosta)	Określane podczas instalacji	Widok	Brak
Friendly Name (Przyjazna nazwa)	Nazwa lokalnego administratora lub opis skanera, wyświetlane na stronie głównej skanerów	Widok/Edycja	Brak
Model	Aperio GT 450 DX	Widok	Brak
Serial Number (Numer seryjny)	Określany podczas instalacji i weryfikowany w trakcie uruchamiania	Widok	Widok
Hardware Version (Wersja sprzętu)	Weryfikowana w trakcie uruchamiania	Widok	Widok
Language (Język)	Kontroluje język używany w menu skanera i język komunikatów	Widok/Edycja	Brak
Additional version information (Dodatkowe informacje o wersji)	Dostępne dla administratora laboratorium na stronie Scanner Information (Informacje o skanerze). Operator może zobaczyć niektóre z tych pól na stronie System Information (Informacje o systemie).	Widok	Widok

Konfiguracja skanera

Należy skorzystać z poniższej tabeli, aby zebrać informacje niezbędne dla każdego skanera w systemie. Po tym, jak przedstawiciel wsparcia technicznego firmy Leica zainstaluje skaner, można zapisać ustawienia, aby zachować je na przyszłość.

Opcja	Opis	Widok/Edycja	
		Administrator	Operator
Images Configuration (Konfiguracja obrazów)			
Scan Scale Factor (Współczynnik skalowania skanu)	Do użytku wewnętrznego. Nie zmieniać, chyba że na polecenie działu wsparcia technicznego firmy Leica Biosystems.	Widok/Edycja	Brak
Hostname (Nazwa hosta)	Nazwa serwera, na którym znajduje się konwerter obrazów DICOM. <ul style="list-style-type: none"> • Użyć nazwy ScannerAdmin (Administrator skanera), jeśli konwerter DICOM zainstalowany jest na serwerze SAM DX. • W przeciwnym wypadku należy użyć nazwy hosta serwera, na którym zainstalowany jest konwerter DICOM. 	Widok/Edycja	Brak
Port	Port, ustawiony w trakcie instalacji dla konwertera DICOM. Domyślnym portem jest 2762.	Widok/Edycja	Brak
Title (Tytuł)	Do użytku wewnętrznego. Nie zmieniać, chyba że na polecenie działu wsparcia technicznego firmy Leica Biosystems.	Widok/Edycja	Brak
File Location (Lokalizacja pliku)	Pełna ścieżka do miejsca udostępnienia pliku, w którym konwerter umieści obrazy po konwersji. Jest to miejsce w sieci, w którym przechowywane są przekonwertowane pliki SVS.	Widok/Edycja	Brak
Image filename format (Format nazwy pliku obrazu)	Ustawia podstawową nazwę pliku dla pliku zeskanowanego obrazu.	Widok/Edycja	Brak
Barcode value identifier (Identyfikator wartości kodu kreskowego)	Ustawia format podstawowy dla kodu kreskowego	Widok/Edycja	Brak
DSR Configuration (Konfiguracja DSR)			
Hostname (Nazwa hosta)	Nazwa hosta serwera, na którym przechowywane będą metadane. (Opcja „File Location” (Lokalizacja pliku) powyżej jest miejscem udostępniania plików, w którym przechowywane są obrazy).	Widok/Edycja	Brak
Port	Zabezpieczony port, używany przez serwer DSR. Domyślnym portem jest 44386.	Widok/Edycja	Brak

Opcja	Opis	Widok/Edycja	
		Administrator	Operator
Event Handling Configuration (Konfiguracja obsługi zdarzeń)			
Hostname (Nazwa hosta)	Nazwa serwera, na którym znajduje się serwer Mirth Connect Server. <ul style="list-style-type: none"> Użyć nazwy ScannerAdmin (Administrator skanera), jeśli serwer Mirth Connect Server zainstalowany jest na serwerze SAM DX. W przeciwnym wypadku należy użyć nazwy hosta serwera, na którym zainstalowana jest używana instancja Mirth dla serwera SAM DX. 	Widok/Edycja	Brak
Log Port (Port dziennika)	Skonfigurowany w trakcie instalacji port, który ma być używany przez Mirth dla danych dziennika. Domyślnym portem jest 6662.	Widok/Edycja	Brak
Event Port (Port zdarzeń)	Skonfigurowany w trakcie instalacji port, który ma być używany przez Mirth dla danych zdarzeń. Domyślnym portem jest 6663.	Widok/Edycja	Brak
PIN Management (Zarządzanie kodami PIN)			
Login Timeout (Limit czasu logowania)	Limit czasu interwału (minuty); skaner blokuje wyświetlacz i klawiaturę sterującą, jeśli przez ten czas operator nie dokona żadnej interakcji. Prawidłową wartością jest dowolna liczba całkowita większa niż zero.	Widok/Edycja	Brak
Edit Settings: Pin (Edytuj ustawienia: kod PIN)	5-cyfrowy kod do odblokowania skanera. Tylko cyfry	Widok/Edycja	Brak
Edit Settings: Opis	Informacje identyfikacyjne dla kodu PIN. Jest to pole zawierające ogólny opis; może zawierać cyfry, litery i znaki interpunkcyjne.	Widok/Edycja	Brak
Time Zone (Strefa czasowa)			
Scanner time zone (Strefa czasowa skanera)	Ustawiane przez administratora serwera SAM DX	Widok/Edycja	Brak

C

Wiązanie certyfikatu SSL z Aperio SAM DX


Dostęp poprzez interfejs użytkownika Aperio SAM DX jest zabezpieczony protokołem SSL. Certyfikaty SSL z podpisem własnym przekazywane są w trakcie instalacji. Aby uniknąć komunikatów bezpieczeństwa ze strony przeglądarki, klienci mogą zastosować własne certyfikaty bezpieczeństwa.

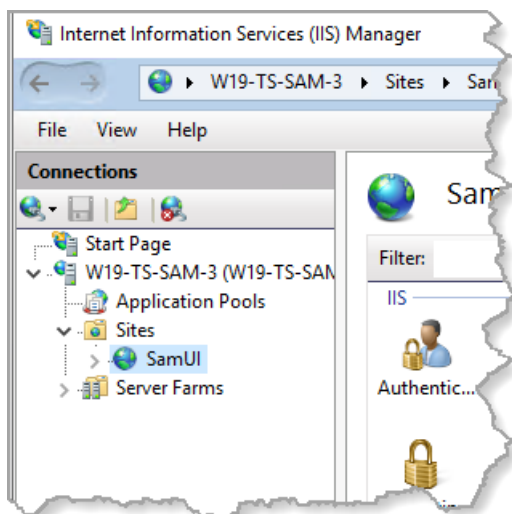
Jeśli instytucja zdecyduje się na stosowanie własnego certyfikatu SSL do zabezpieczania interfejsu użytkownika Aperio SAM DX, taki certyfikat SSL musi zostać zaimportowany i powiązany z aplikacją SAM DX.

Niniejsza sekcja omawia, w jaki sposób należy zaktualizować powiązanie certyfikatu SSL, aby zabezpieczyć interfejs użytkownika SAM DX w Microsoft IIS.

Należy zaimportować certyfikat SSL do Microsoft IIS według instrukcji dostawcy certyfikatu SSL. Następnie należy postępować zgodnie z instrukcjami poniżej, aby powiązać certyfikat z aplikacją SAM DX.

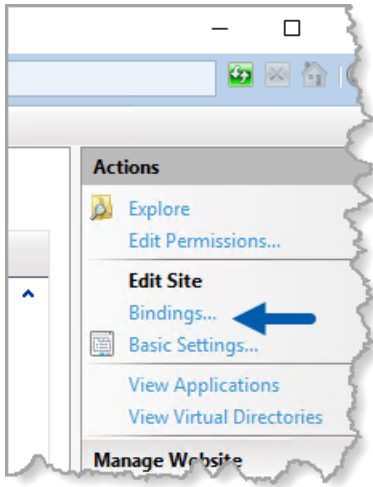
Przypisywanie certyfikatu SSL do witryny internetowej

1. Na serwerze aplikacji SAM DX należy kliknąć przycisk Windows **Start**  i wpisać **inetmgr**.
2. Przypisać certyfikat SSL do witryny internetowej poprzez rozwinięcie podsekcji **Sites** (Witryny) w menu **Connections** (Połączenia) po lewej stronie i wybranie swojej witryny internetowej:

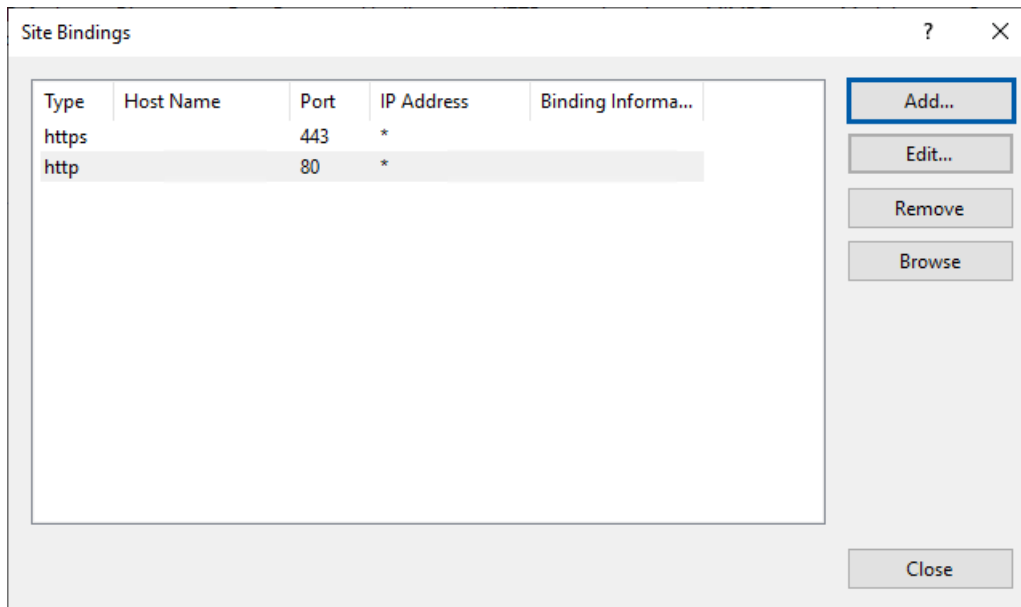


Wiązanie certyfikatu SSL

1. W panelu Actions (Akcje) po prawej stronie znaleźć menu **Edit Site** (Edytuj witrynę) i wybrać opcję **Bindings** (Powiązania).



2. Po prawej stronie okna Site Bindings (Powiązania witryn) kliknąć **Add** (Dodaj):



3. W oknie Add Site Binding (Dodaj powiązanie witryny) należy zmodyfikować poniższe pola:
 - a. W polu Type (Typ) wybrać **https**.
 - b. W polu IP address (Adres IP) wybrać adres IP witryny internetowej lub opcję **All Unassigned** (Wszystkie nieprzydzielone).
 - c. W polu Port wpisać 443 (domyślny).
 - d. W polu SSL certificate (Certyfikat SSL) wybrać wcześniej zaimportowany certyfikat, który można zidentyfikować na podstawie przyjaznej nazwy.



Jeśli na serwerze znajduje się wiele certyfikatów SSL, należy zaznaczyć pole **Require Server Name Indication** (Wymagaj wskazania nazwy serwera).

Edit Site Binding

Type: **A** https

IP address: **B** All Unassigned

Port: **C** 443

Host name:

Require Server Name Indication

Disable HTTP/2

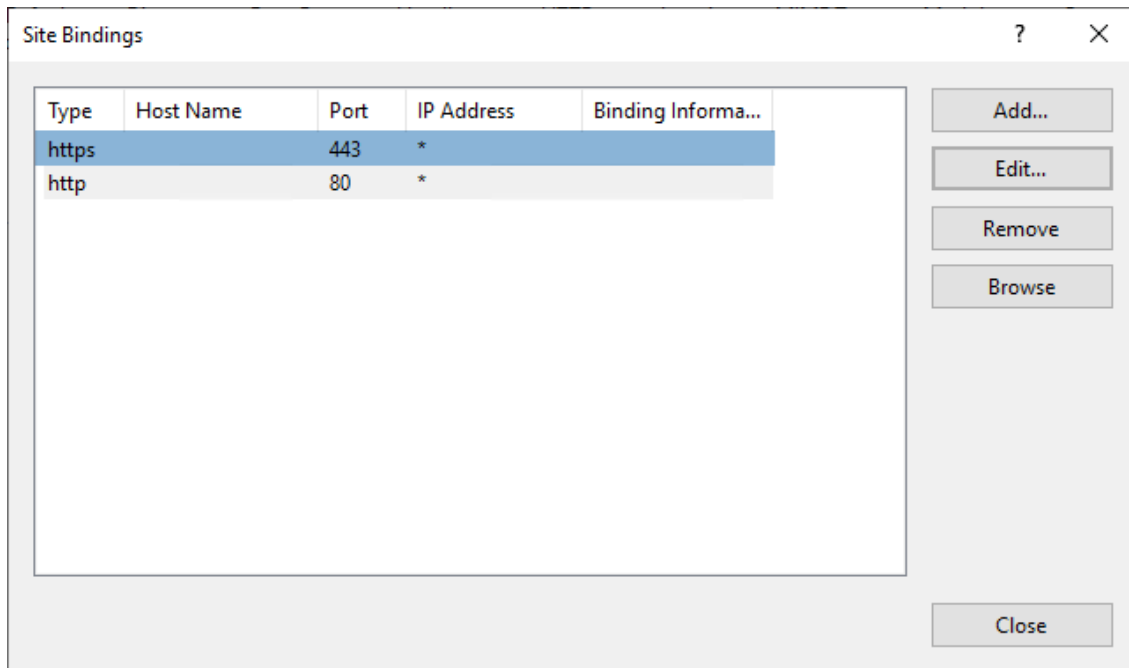
Disable OCSP Stapling

SSL certificate: **D** Not selected

Select... View...

OK Cancel

4. Kliknąć **OK**, aby nowy wpis https pojawił się w oknie Site Bindings (Powiązane witryny):



Certyfikat jest teraz zainstalowany, a interfejs użytkownika SAM DX powinien być teraz dostępny poprzez HTTPS.

Indeks

A

- adres MAC 43
 - wyświetlanie 30
- alerty włamań 32
- architektura 15

C

- certyfikat SSL
 - przypisywanie do SAM DX 46
 - uzyskiwanie 46
 - wiązanie 47
- certyfikat, SSL. *Zob.* certyfikat SSL

D

- dane kontaktowe działów obsługi klienta 8
- DICOM 15, 18
 - konfigurowanie wyjścia DICOM 28
- dokumenty 12
- DSR 16
 - ustawienia 23, 30, 44
- dzienniki zdarzeń 32

F

- format nazwy pliku 26
- format nazwy pliku obrazu, modyfikowanie 26

G

- gotowe komercyjne oprogramowanie 40

H

- hasła 33, 34, 36

I

- informacje o systemie 30
 - Strona Settings (Ustawienia) 22
 - Uzyskać dostęp do strony Info (Informacje) 21
- interfejs użytkownika 13

K

- kod kreskowy 26
 - identyfikator wartości 26
 - wymaga 26, 27
- konfiguracja sieciowa 16
 - system 18

L

- limit czasu 27, 45
- limit czasu logowania 27, 45
 - najlepsze praktyki 27

N

- nazwa hosta
 - konwerter DICOM 44
 - podstawowe ustawienia skanera 43
 - serwer Mirth Connect 45
 - skaner, wyświetlanie 30

O

- obsługa 40
- ochrona cyberbezpieczeństwa
 - DSR, ochrona 39
 - normy informatyczne 39
 - rejestrwanie dostępu 39
 - umożliwienie listowania 39
 - zabezpieczenia administracyjne 39
 - zabezpieczenia fizyczne 39
- odblokowywanie kont użytkowników 35

P

- PIN 27, 45
 - konfiguracja 27
 - limit czasu 27
 - zarządzanie 24, 27
- PIN, bieżący widok 31
- pliki dzienników 32
 - pobieranie 32
- podstawowe ustawienia skanera 43
- poprawki cyberbezpieczeństwa 40
- powiązane dokumenty 12
- przewidziane zastosowanie 11

R

- Rola administratora 34
- Rola Lab Admin (Administrator laboratorium) 34
- Rola Operator 33
- role 33
- role użytkowników 33
 - definicje 33
 - dodawanie 34
 - edytowanie 35
 - hasła 34
 - odblokowywanie kont 35
- Rola Lab Admin (Administrator laboratorium) 34
- Rola Operator 33
- usuwanie 35
- rozwiązywanie problemów 41

S

- SAM DX 11
 - ekran główny 13
 - funkcje 11
 - konfiguracja sieciowa 16
 - logowanie 12
 - rozwiązywanie problemów 41
 - zarządzanie użytkownikami 33
- ścieżki komunikacji danych 17
 - schemat 17
- serwer Digital Slide Repository (DSR) 16

- skaner
 - dzienniki zdarzeń 32
 - strefa czasowa 45
- SSL 16, 46
- strefa czasowa 24, 45

T

- typy obrazów 15

U

- umożliwienie listowania 39
- ustawienia
 - strona Images 23
- ustawienia konfiguracji
 - Skaner 23
- ustawienia obrazów 23
- ustawienia obsługi zdarzeń 24, 31, 45
- ustawienia serwera Mirth 31
- ustawienia skanera 20
- użytkownicy, bieżący widok 31

W

- wymogi dotyczące przepustowości sieci 16

Z

- zarządzanie kodami PIN
 - ustawienia 45

